В. Ю. ШЕВЦОВ
Е. В. БУЛГАКОВА
А. Н. КУБАНКОВ

ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОС СЕМЕЙСТВА LINUX

С ИСПОЛЬЗОВАНИЕМ ПО SECRET NET LSP

«Инфра-Инженерия»

В. Ю. Шевцов, Е. В. Булгакова, А. Н. Кубанков

ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОС СЕМЕЙСТВА LINUX С ИСПОЛЬЗОВАНИЕМ ПО SECRET NET LSP

Учебно-методическое пособие

Москва Вологда
«Инфра-Инженерия»
2025

УДК 004.7
ББК 32.973
Ш37

Рецензенты:
кандидат физико-математических наук, доцент, заведующий кафедрой информационной безопасности института приоритетных технологий Волгоградского государственного университета *Какорина О. А.*;
доктор физико-математических наук, профессор, профессор кафедры информационной безопасности Финансового университета при Правительстве РФ *Крылов Г. О.*

Шевцов, В. Ю.

Ш37 Обеспечение комплексной безопасности ОС семейства Linux с использованием ПО Secret Net LSP : учебно-методическое пособие / В. Ю. Шевцов, Е. В. Булгакова, А. Н. Кубанков. – Москва ; Вологда : Инфра-Инженерия, 2025. – 48 с. : ил., табл.

ISBN 978-5-9729-2223-9

Рассматривается установка, настройка и эксплуатация средства защиты для операционных систем Linux – Secret Net LSP. Особое внимание уделено таким функциям, как разграничение доступа, замкнутая программная среда и межсетевое экранирование. Лабораторные работы состоят из теоретической и практической части, контрольных вопросов.

Для студентов уровня бакалавриата и специалитета группы специальностей 10.00.00 «Информационная безопасность».

УДК 004.7
ББК 32.973

ISBN 978-5-9729-2223-9

Введение

Несмотря на высокую долю проприетарных операционных систем (ОС) в России (в основном ОС семейства Windows), актуальным является переход на ОС отечественных разработчиков в результате выбранного курса на импортозамещение в стране. При этом следует учесть, что большинство таких ОС разработано на базе ядра Linux. Также часть организаций использует свободно-распространяемые системы, либо зарубежные проприетарные системы на их основе (особенно в серверной инфраструктуре).

Встроенный функционал защиты на уровне ОС Linux не является исчерпывающим, особенно при учёте требований регуляторов. Для реализации полноценной защиты рабочих станций необходимо использование СЗИ от НСД. Для ОС Linux такие системы чаще всего предоставляют следующее:

- контроль входа пользователей в систему (в том числе с использованием аппаратных средств защиты);
- разграничение доступа ресурсам компьютера (в том числе внешним);
- безвозвратное удаление данных и затирание остаточной информации;
- контроль целостности ресурсов компьютера;
- создание замкнутой программной среды;
- межсетевое экранирование;
- регистрация и мониторинг событий безопасности;
- аудит действий субъектов и сетевых соединений.

Одним из средств, предоставляющих перечисленный функционал, является Secret Net LSP. Важным преимуществом при использовании данного СЗИ от НСД является наличие сертификата ФСТЭК.

Настоящее учебное пособие предназначено для студентов по направлениям группы специальностей 10.00.00 «Информационная безопасность» в рамках освоения дисциплины «Программно-аппаратные средства защиты информации».

В пособии рассматриваются теоретические и практические аспекты использования СЗИ от НСД Secret Net LSP 1.12, что позволяет обеспечить надежную защиту рабочих станций на базе ОС Linux в соответствии с нормативными требованиями.

Подготовка к лабораторным работам

Перед выполнением лабораторных работ необходимо выполнить следующие действия:

1. Установить VirtualBox новейшей версии (возможно использование другого ПО виртуализации).

2. Создать виртуальную машину для выбранной ОС Linux со следующими параметрами: ОЗУ не менее 4 ГБ, 2 динамически расширяющихся образа жесткого диска с объемом, рекомендуемым для выбранной ОС (при этом для системы защиты должно остаться не менее 1 ГБ свободного пространства на системном диске).

3. Настроить сетевой интерфейс в режиме NAT, общие папки, контроллер USB.

4. Произвести установку выбранной ОС Linux. Во время установки рекомендуется отключить сетевой интерфейс. В случае отсутствия поддерживаемой версии ОС в распространяемых дистрибутивах необходимо произвести изменение ядра до требуемого с использованием репозиториев по умолчанию.

5. Обновить пакеты программ.

6. Произвести установку гостевых дополнений (либо другое специализированное ПО для интеграции с системой виртуализации).

7. Проверить наличие следующего прикладного ПО (произвести установку в случае отсутствия):

- LibreOffice Calc (или аналог);
- Mozilla Firefox;
- Thunderbird (или аналог);
- Калькулятор;
- Текстовый редактор;
- GIMP (или аналог);

- VLC Media Player (или аналог);
- Просмотр изображений;
- GParted;
- LibreOffice Draw.

Лабораторная работа № 1

Тема: Система защиты информации «Secret Net LSP 1.12».

Цель: Изучить общие сведения о СЗИ Secret Net LSP.

Теоретическая часть

Назначение

Программный продукт Secret Net LSP 1.12 предназначен для защиты от НСД к информационным ресурсам компьютеров, функционирующих на компьютерах, удовлетворяющих требованиям, приведенным в таблице 1.

Таблица 1. Системные требования Secret Net LSP 1.12

Операционная система	- Альт 8 СП (версия ядра 5.10.110-alt0.c9f.2, DE: MATE); - Альт Рабочая Станция 9.2 (версия ядра 5.10.118-un-def-alt1, DE: MATE); - Альт Сервер 9.2 (версия ядра 5.10.118-un-def-alt1, DE: MATE); - Альт Рабочая Станция 10 (версия ядра 5.10.82-std-def-alt1, DE: MATE); - Альт Сервер 10 (версия ядра 5.10.82-std-def-alt1, DE: MATE); - Альт К 10 (версия ядра 5.15.37-un-def-alt1, DE: MATE); - Ред ОС 7.3 (версия ядра 5.15.35-1.el7.x86_64, DE: MATE); - Astra Linux Common Edition 2.12.44 (версия ядра 5.10.0-1038.40 generic/hardned, 5.4.0-71 generic/hardned, 4.15.3-141 generic/hardned, DE: FLY); - Astra Linux Special Edition 1.7 (версия ядра 5.10.0-1045 generic/hardned, 5.4.0-81 generic/hardned, DE: FLY) и обновления № 2022-№ 0318SE17MD, № 2022-0407SE17MD; - CentOS 7.9 (версия ядра 3.10.0-1160.66.1.el7.x86_64, DE: GNOME); - CentOS 8.5 (версия ядра 4.18.0-348.7.1.el8_5.x86_64, DE: GNOME); - Debian 11.3 (версия ядра 5.10.0-13-amd64, DE: GNOME);

Окончание таблицы 1

	- Oracle Linux 8.6 (версия ядра 4.18.0-372.9.1.el8.x86_64, 5.4.17-2136.307.3.4.el8uek.x86_64); - Red Hat Enterprise Linux 7.9 (версия ядра 3.10.0-1160.66.1.el7.x86_64, DE: GNOME); - Red Hat Enterprise Linux 8.5 (версия ядра 4.18.0-348.7.1.el8_5.x86_64, DE: GNOME); - Red Hat Enterprise Linux 8.6 (версия ядра 4.18.0-372.9.1.el8.x86_64, DE: GNOME); - SUSE Linux Enterprise Server 12 SP5 (версия ядра 4.12.14-120-default); - SUSE Linux Enterprise Server 15 SP3 (версия ядра 5.3.18-57-default); - Ubuntu 18.04 (версия ядра 5.4.134-19-generic, DE: GNOME); - Ubuntu 18.04.6 (версия ядра 5.4.0-110-generic, DE: GNOME); - Ubuntu 20.04.3 (версия ядра 5.10.65+yc0.406, 5.11.0-27-generic, DE: GNOME); - Ubuntu 20.04.4 (версия ядра 5.13.0-41-generic, DE: GNOME); - Ubuntu 22.04 (версия ядра 5.15.0-30-generic, DE: GNOME)
Процессор	В соответствии с операционной системой, установленной на компьютер, минимально 2 ядра
Оперативная память	Минимально – 2 ГБ. Рекомендуется – 4 Гбайт (при использовании подсистемы замкнутой программной среды или межсетевого экранирования)
Жесткий диск	Свободное место – не менее 1 ГБ

Основные функции

Secret Net LSP реализует следующие основные функции:

- контроль входа пользователей в систему, в том числе с использованием аппаратных средств защиты;

- разграничение доступа пользователей к защищаемым ресурсам (файлам, каталогам) компьютера;

- разграничение доступа пользователей к шинам USB, SATA, IEEE 1394 и подключаемым к ним устройствам;

- уничтожение (затирание) содержимого файлов при их удалении;
- очистка освобождаемых областей оперативной памяти компьютера и запоминающих устройств (жестких дисков, внешних запоминающих устройств);
- контроль целостности ключевых компонентов Secret Net LSP и объектов файловой системы;
- создание замкнутой программной среды для пользователей;
- регистрация событий безопасности в журналах;
- контроль действий пользователей, связанных с доступом к файлам, устройствам и узлам вычислительной сети;
- проведение аудита действий субъектов (пользователей, процессов) с объектами файловой системы и аудита сетевых соединений.

Защитные механизмы

Защитные механизмы – это программные и аппаратные средства, предназначенные для реализации защитных функций системы Secret Net LSP. В СЗИ представлены следующие механизмы защиты:

1. Механизм защиты входа в систему:
- идентификация и аутентификация пользователей;
- режимы входа;
- блокировка входа в систему;
- блокировка учетных записей;

2. Механизм разграничения доступа и защиты ресурсов:
- права доступа UNIX;
- списки контроля доступа POSIX ACL;
- механизм разграничения доступа к устройствам;

3. Механизм контроля целостности:
- объекты и параметры контроля;
- методы контроля;
- регистрация событий;

- реакция СЗИ на нарушение целостности объектов;
- настройка механизма;

4. Механизм замкнутой программной среды:

- режимы работы механизма;
- регистрация событий;
- белый список пользователей и групп;
- список исключений для ресурсов;
- правила;
- механизм регистрации событий;
- механизм затирания остаточной информации.

Архитектура

Secret Net LSP имеет модульную архитектуру и включает в свой состав следующие основные подсистемы:

1. Подсистема локального управления. Предназначена для управления подсистемами, входящими в состав СЗИ, и контроля их работоспособности.

2. Подсистема идентификации и аутентификации. Управляет работой механизма защиты входа пользователей в систему.

3. Подсистема разграничения доступа к файлам и каталогам. Реализует дискреционную модель разграничения доступа субъектов (пользователей, процессов) к объектам файловой системы.

4. Подсистема разграничения доступа к устройствам. Реализует дискреционную модель разграничения доступа пользователей к USB-флеш-накопителям.

5. Подсистема контроля целостности. Осуществляет контроль целостности программных компонентов комплекса средств защиты (КСЗ) и объектов файловой системы. Осуществляет тестирование работоспособности модулей всех КСЗ по требованию администратора и самотестирование до запуска компонентов СЗИ.

6. Подсистема журналирования. Осуществляет сбор сведений о событиях, зарегистрированных в других подсистемах, и формирование системного журнала и журнала аудита.

7. Подсистема аудита. Предназначена для работы с журналами и настройки регистрации событий и правил аудита.

8. Подсистема очистки памяти. Осуществляет очистку затиранием выделенных или перераспределенных участков оперативной памяти и освобождаемых участков на жестких дисках или внешних устройствах.

Порядок установки

Перед установкой Secret Net LSP необходимо убедиться в выполнении следующих требований:

- на компьютере установлена только одна поддерживаемая операционная система с одним ядром;
- ядро операционной системы должно входить в список ядер, заявленных как поддерживаемые компанией – разработчиком СЗИ, и соответствовать устанавливаемому дистрибутиву Secret Net LSP.

Для установки Secret Net LSP:

1. Вставьте установочный носитель Secret Net LSP в устройство чтения. Запустите программу эмулятора терминала.

2. Перейдите в каталог, соответствующий установленной ОС. Выполните следующие команды:

apt update

apt install ./<пакет sn-lsp>

3. Перезагрузите компьютер. После перезагрузки на компьютере будет отключена мандатная система контроля доступа (SELinux, Apparmor, Tomoyo Linux, RSBAC и пр.).

4. Для работы с лицензиями используется утилита snlicensectl (путь: /opt/secretnet/bin). Чтобы выбрать файл лицензии, выполните в терминале: */opt/ /secretnet/bin/snlicensectl --change <путь до файла с лицензией>*

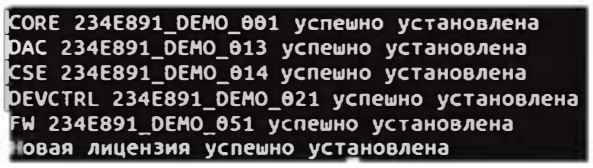

Рисунок 1 – Результат установки лицензии (демонстрационная версия)

Управление подсистемами

и утилита управления параметрами политик

Ключевой компонент Secret Net LSP – подсистема управления. В её состав входят:

- утилиты загрузки и инициализации;
- плагины безопасности;
- CLI-утилиты.

В данной лабораторной работе будут рассмотрены следующие утилиты:

- snpolctl (управление параметрами политик);
- snbckctl (резервное копирование и восстановление).

Синтаксис команд утилиты snpolctl имеет следующий формат:

snpolctl <флаг> [<параметр (плагин)>] [<флаг>] [<политика>]
[<параметр>] [<значение>]

Резервное копирование настроек

Для выполнения операций резервного копирования и восстановления используется утилита snbckctl. Данная утилита работает со следующими объектами:

- данные о пользователях и группах;
- база данных настроек Secret Net LSP;
- содержимое журналов.

Порядок работы с данной утилитой следующий:

1. Резервное копирование (возможно для определенных объектов, но без их указания будет выполнено полностью):

snbckctl -b

Конфигурация по следующему пути: /opt/secretnet/usr/backup/<ID>, где <ID> – это сгенерированный системой номер резервной копии.

2. Для проверки, что резервная копия была создана, выполните:

snbckctl -l

3. Экспорт необходимой резервной копии:

snbckctl -e -i <ID_резервной_копии>

После выполнения команды появится файл архива (с расширением .tar.gz) с резервной копией настроек в следующем каталоге: /opt/secretnet/usr/backup/.

4. Импорт резервной копии (предварительно необходимо поместить архив с резервной копии в каталог /opt/secretnet/usr/backup/):

snbckctl -m -i <ID_резервной_копии>

где ID_резервной_копии – это имя файла архива без расширения.

5. Восстановление настроек из импортированной резервной копии:

snbckctl -r -i <ID_резервной_копии>

Механизм затирания остаточной информации
и очистка оперативной памяти

По умолчанию после установки в Secret Net LSP автоматическое затирание выключено, так как использование этого механизма приводит к повышенной нагрузке на файловую систему и жесткие диски.

Действие механизма заключается в очистке освобождаемых областей памяти путем выполнения в них однократной произвольной записи.

Затирание остаточной информации на файловой системе происходит при выполнении следующих операций с файлами:

- удаление (unlink);
- переименование в рамках перемещения (rename);
- модификация размера файла (truncate).

Предусмотрены два режима затирания на жестких дисках и внешних запоминающих устройствах: синхронный и асинхронный.

В синхронном режиме модуль ядра перехватывает запросы к файловым системам на освобождение блоков данных, осуществляет запись в них маскирующей информации и помечает их как свободные.

В асинхронном режиме предусмотрено отложенное затирание удаляемых файлов. Модуль ядра перехватывает запросы к файловым системам на удаление файлов данных, перемещает их в специальные каталоги (корзины) для дальнейшей очистки сервисом затирания.

Для включения механизма необходимо установить значение параметра «Сервис безопасного удаления» равным 1, используя утилиту snpolctl (плагин системные сервисы):

snpolctl -p service_mgr -c services,sntrashd,1

Чтобы включить очистку оперативной памяти, необходимо выполнить следующую команду (плагин модули ядра):

snpolctl -p control -c memory,mode,1

Работа с журналами

Операции с журналами в Secret Net LSP производятся при помощи утилиты snjrnl, имеющей следующие возможности:

- просмотр записей системного журнала и журнала аудита;
- удаление записей из базы данных журналов;
- экспорт записей журналов в файл;
- импорт записей журналов из файла;
- сортировка событий.

Для включения механизма необходимо установить значение параметра «Сервис журналирования» равным 1, используя утилиту snpolctl (плагин системные сервисы):

snpolctl -p service_mgr -c services,snjournald,1

Утилита snjrnl имеет следующие ключи:

1. -h [--help] – справочная информация об утилите;
2. -S [--syslog] – работа с системными журналами;
3. -A [--audit] – работа с журналами аудита;

4. -w [--view] – просмотр выбранных записей. При отсутствии временного периода производится выбор записей за текущий день;

5. -e [--export]=имя_файла – экспорт журналов в файл;

6. -d [--delete] – удаление экспортированных записей;

7. -i [--import]=имя_файла – импорт журналов из файла;

8. -D [--delete-only] – удаление записей;

9. -f [--from]=дата – работа с записями, созданными не ранее указанной даты;

10. -t [--to]=дата – работа с записями, созданными не позднее указанной даты;

11. -p [--priority]=приоритет – работа с записями заданного приоритета (для системных журналов);

12. -M [--message]=текст – работа с записями, содержащими указанную строку;

13. -u [--user]=пользователь – работа с записями для заданного пользователя (для журналов аудита);

14. -g [--group]=группа – работа с записями для заданной группы (для журналов аудита);

15. -a [--app]=приложение – работа с записями для заданного приложения;

16. -o [--object]=объект – работа с записями для заданного объекта (для журналов аудита);

17. -r [--result]=результат – работа с записями для заданного результата (0 – ошибка; 1 – успешно);

18. -v [--verbose] – отображение сообщений отладки.

Примеры команд для работы с журналами:

- отобразить записи системных журналов за текущий день: *snjrnl -S -w*
- отобразить записи базы данных аудита за указанный период: *snjrnl -S -w -f=01.01.2024 -t=03.01.2024*
- очистить записи системного журнала: *snjrnl -S -D*

Практическое задание

1. Используя терминал, произведите обновление установленных пакетов.

2. Произведите установку Secret Net LSP.

3. Произведите установку лицензии.

4. Проверьте статус лицензии. Для этого используйте утилиту snlicensectl с флагом -s [--status].

5. Выполните резервное копирование настроек Secret Net LSP.

6. Включите механизм затирания остаточной информации.

7. Включите очистку оперативной памяти.

8. Отобразите состояние политик программы. Для этого используйте утилиту snpolctl с флагом -l [--list].

9. Произведите блокировку системы. Для этого используйте утилиту snpolctl (плагин system) с флагом -p [--plugin] и параметром system_lock (значение параметра 1).

10. Проверьте возможность входа в систему пользователем без прав администратора. Отключите блокировку системы (выполняется аналогично включению блокировки, но со значением параметра system_lock, равным 0).

11. Отобразите записи журнала аудита за время выполнения лабораторной работы.

Контрольные вопросы

1. Назначение Secret Net LSP.

2. Системные требования Secret Net LSP.

3. Основные функции Secret Net LSP.

4. Защитные механизмы Secret Net LSP.

5. Архитектура Secret Net LSP.

6. Порядок установки Secret Net LSP.

7. Утилита управления параметрами политик.

8. Резервное копирование настроек.

9. Механизмы затирания остаточной информации и очистки оперативной памяти в Secret Net LSP.

10. Работа с журналами.

Лабораторная работа № 2

Тема: Разграничение доступа пользователей к ресурсам в ПАСЗИ «Secret Net LSP 1.12».

Цель: Настройка дискреционного разграничения доступа в Secret Net LSP и механизмов входа в систему.

Теоретическая часть

Управление параметрами безопасности паролей и входа пользователей

Для настройки сложности и времени действия паролей пользователей используется утилита snpolctl и плагин users и одноимённая политика. Политика users имеет следующие параметры:

- min_passwd_size – минимальная длина для нового пароля (от 6 до 16 символов);

- passwd_strength – включить или отключить требования к безопасности пароля;

- max_days – максимальное время действия пароля (в днях от -1 до 9999);

- min_days – минимальное время действия пароля (в днях от 0 до 999999);

- warn_days – время до предупреждения о необходимости смены пароля (в днях от 0 до 999999);

- inactive_days – время действия просроченного пароля (в днях от -1 до 999999).

Примеры команд для управления параметрами безопасности паролей:

Включить требования к безопасности пароля: *snpolctl -p users -c users, passwd_strength,1*

Установить максимальное время действия пароля, равное 30 дням: *snpolctl -p users -c users,max_days,30*

Установить время действия просроченного пароля, равное 3 дням: *snpolctl -p users -c users,inactive_days,3*

Параметры входа пользователя также настраиваются утилитой snpolctl, но с использованием плагина token_mgr и политики authentication. Параметры политики (без учёта настроек аппаратных идентификаторов):

- state – состояние политики (включено или отключено);

- deny – количество неудачных попыток входа (от 0 до 999999);

- unlock_time – время блокировки учётной записи при превышении заданного количества неудачных попыток аутентификации (от 0 до 90 минут);

- lock_delay – период неактивности до блокировки экрана (от 0 до 999999 минут);

- last_log – уведомление пользователя о последнем успешном входе (включено или отключено).

Примеры команд для управления параметрами входа пользователей:

- установить количество неудачных попыток ввода равным 5: *snpolctl -p token_mgr -c authentication,deny,5*

- установить время блокировки учётной записи при превышении 7 неудачных попыток аутентификации: *snpolctl -p token_mgr -c authentication, unlock_time,7*

- установить время неактивности до блокировки экрана равным 10 минутам: *snpolctl -p token_mgr -c authentication,lock_delay,10*

- включить уведомление пользователя о последнем успешном входе: *snpolctl -p token_mgr -c authentication,last_log,1*

Дискреционное разграничение доступа

Подсистема позволяет осуществлять контроль доступа пользователей к объектам файловой системы на основе прав доступа UNIX, а также списков POSIX ACL для объектов.

Состав подсистемы:

- механизмы разграничения прав доступа на уровне модуля ядра;
- CLI-утилита управления;
- плагин сервиса управления.

Механизмы на уровне модуля ядра обеспечивают:

- взаимодействие с ядром ОС;
- перехват обращений к файловой системе;
- контроль доступа субъектов к объектам на основании ACL из xattrs файловой системы.

CLI-утилита управления использует следующие системные команды для настройки доступа:

- chmod, chown, chgrp, chfn (для DAC);
- setfacl, getfacl (ACL).

Активация механизма дискреционного разграничения доступа на уровне СЗИ реализуется утилитой snpolctl с использованием плагина system и политики control (параметр access_control).

Управление доступом к устройствам

Для разграничения и контроля прав доступа к устройствам используется утилита sndevctl. Данная утилита содержит следующие ключи:

1) -l [--list] – список шин и устройств;
2) -r [--rules] – текущие правила для шин и устройств;
3) -a [--add] – добавление нового устройства;
4) -m [--model] – добавление модели;
5) -d [--delete] – удаление модели или устройства;
6) -s [--set] – установление параметров шины или устройства;
7) -c [--config] – проверка и утверждение аппаратной конфигурации;
8) -i [--import] – импорт устройства или модели.

Возможные режимы правил работы для устройств:

- not-control – устройство не контролируется;
- fixed – включён режим контроля устройства (при изменениях статуса устройства возникает критичное событие и необходимо утверждение новой аппаратной конфигурации);

- lock – блокировка компьютера при изменении состояния устройства;

- enabled – разрешённое устройство;

- disable – запрещённое устройство.

Примеры команд для утилиты приведены ниже:

Детализированный список USB-устройств: *sndevctl --lv --bus-id=usb*

Установка прав доступа к устройству «Kingston» (для пользователя user1 – только чтение, для остальных – чтение и запись): *sndevctl --set --dev-id=1 --label=«Kingston» --user=user1:read --default=write*

Установка прав доступа к USB-шине (для пользователя test1 – чтение и запись, для остальных – нет доступа): *sndevctl --set --bus-id=usb --user=test1:write --default=none*

Контроль целостности

Настройка контроля целостности производится с использованием утилиты snaidectl. Данная утилита содержит следующие ключи:

1. -c [--check] – проведение контроля целостности;

2. -i [--init] – инициализация базы данных контроля целостности;

3. -l [--list] – отображение файлов с контролем целостности;

4. -s [--set] – включение контроля целостности для выбранных файлов;

5. -u [--unset] – отключение контроля целостности для выбранных файлов;

6. -U [--unset-all] – отключение контроля целостности;

7. -v [--view-schedule] – текущие настройки расписания контроля целостности;

8. -a [--add-schedule-entry] – добавление записи контроля целостности в расписание;

9. -d [--delete-schedule-entry] – удаление записи контроля целостности;

10. -r [--real-time] – включение контроля целостности в реальном времени в запросе (используется совместно с ключом --set).

Примеры команд для утилиты приведены ниже:

Выполнение контроля целостности: *snaidectl –check*

Отобразить правила контроля целостности для файла: *snaidectl --list=file1*

Включение контроля для файла file1 с флагом NORMALLOCK (протоколирование события при изменении файла и блокировка системы), для папки используется аналогичная команда: *snaidectl --set file1=NORMALLOCK*

Пример выше с добавлением контроля целостности в реальном времени: *snaidectl --set file1=NORMALLOCK --real-time*

Аудит действий пользователей

Аудит в Secret Net LSP реализуется при помощи утилиты snauditctl. Подсистема аудита предназначена для отслеживания действий субъектов (пользователи, группы, процессы) и операций с объектами (файлы, каталоги, сетевые соединения, устройства).

Для включения механизма необходимо установить значение параметра «Сервис аудита» равным 1, используя утилиту snpolctl (плагин системные сервисы).

snpolctl -p service_mgr -c services,snauditd,1

Утилита snjrnl имеет следующие ключи:

1. -l [--list] – текущие правила аудита;

2. -A [--add] – создание правила аудита;

3. -m [--modify]=ID – изменения правила с идентификатором ID;

4. -r [--result]=РЕЗУЛЬТАТ – результат выполнения действия (0 – любой; 1 – успех; 2 – неудача);

5. -d [--delete]=ID – удаление правила с идентификатором ID;

6. -D [--delete-all] – удаление всех правил;

7. -c [--comment]=ТЕКСТ – задание текстового комментария для правила. Используется с ключами «-A» и «-m»;

8. -u [--user]=ПОЛЬЗОВАТЕЛЬ,… – список пользователей, к которым применяется правило;

9. -g [--group]=ГРУППА,… – список групп, к которым применяется правило;

10. -o [--object]=ОБЪЕКТ – контролируемый объект (файл или каталог). Данная команда выполняется отдельно для каждого объекта;

11. -a [--action]=ДЕЙСТВИЕ,… – разделенный запятыми список действий, отслеживаемых правилом.

Примеры команд для утилиты приведены ниже:

Добавление правила для записи событий чтения подключённых устройств (кроме системного диска): *snauditctl -A -o /dev -a openr*

Добавление правила для записи событий операций записи в указанной папке: *snauditctl -A -o /home -a openr*

Практическое задание

1. Создайте пользователей worker1, worker2.

2. Настройте требования к паролям следующим образом (таблица № 2).

Таблица 2. Требования к паролям

Вариант	Минимальная длина (символов)	Требования к безопасности	Срок действия (дней)	Время до предупреждения о смене пароля (дней)	Время действия просроченного пароля
1	8	есть	90	80	7
2	12	нет	120	100	3
3	10	есть	60	45	5
4	8	нет	40	35	0
5	8	нет	30	27	0
6	12	нет	180	160	9
7	10	есть	70	50	4
8	9	есть	80	65	2
9	11	есть	95	85	10
10	9	нет	45	40	–1

3. Настройте параметры входа пользователей в соответствии с таблицей 3.

Таблица 3. Параметры входа пользователей

Вариант	Максимальное количество неудачных попыток входа	Время блокировки учётной записи (минут)	Период неактивности до блокировки экрана (минут)	Уведомление о последнем успешном входе
1	3	3	10	включено
2	7	4	30	отключено
3	5	5	15	включено
4	3	3	20	отключено
5	3	7	25	отключено
6	7	8	25	отключено
7	5	4	15	включено
8	4	3	10	включено
9	6	5	5	включено
10	4	7	20	отключено

4. Создайте пользователей test1, test2.

5. Создать следующие директории на несистемном диске: docs, publisher, fork, business.

6. Задайте дискреционный доступ для директорий в соответствии с таблицей 4.

Таблица 4. Настройки дискреционного доступа

Директория	worker1	worker2	test1
Вариант 1, 2			
.\docs	З	З	ПД
.\publisher	ПД	Д	Д
.\fork	ПД	ЗД	Д
.\business	ЗД	ЗД	ПД
Вариант 3, 4			
.\docs	Д	ЗД	ПД
.\publisher	Д	Д	ПД

Окончание таблицы 4

Директория	worker1	worker2	test1
.\fork	ПД	ПД	Д
.\business	З	З	ПД
Вариант 5, 6			
.\docs	ЗД	ЗД	ПД
.\publisher	ПД	ПД	ПД
.\fork	Д	З	Д
.\business	З	З	ПД
Вариант 7, 8			
.\docs	Д	Д	З
.\publisher	ПД	ПД	ПД
.\fork	ЗД	ПД	ЗД
.\business	Д	Д	ПД
Вариант 9, 10			
.\docs	З	З	Д
.\publisher	Д	ПД	ПД
.\fork	З	З	Д
.\business	З	ЗД	Д

где ПД – полный доступ, З – запись, Д – чтение, ЗД – запрет доступа.

7. Активируйте механизм дискреционного разграничения доступа на уровне СЗИ.

8. Проверьте возможность выполнения операций в соответствии с таблицей 5.

Таблица 5. Задание к п. 7

Вариант	Пользователь	Чтение	Изменение	Перемещение файла
1	worker1	.\docs	.\business*.txt	.\docs
2	worker2	.\fork	.\publisher*.txt	.\docs
3	worker1	.\business	.\docs*.txt	.\business
4	worker2	.\docs	.\publisher*.txt	.\business
5	worker1	.\docs	.\fork*.txt	.\business

Окончание таблицы 5

Вариант	Пользователь	Чтение	Изменение	Перемещение файла
6	worker2	.\docs	.\business*.txt	.\fork
7	worker1	.\fork	.\docs*.txt	.\business
8	test1	.\fork	.\publisher*.txt	.\docs
9	worker1	.\business	.\publisher*.txt	.\fork
10	worker2	.\business	.\publisher*.txt	.\fork

9. Согласно варианту (таблица 6) запретите доступ пользователю к съемным USB-устройствам. Проверьте возможность использования одного из подключённых USB-устройств этим пользователем.

Таблица 6. Задание к п. 7

Вариант	Пользователь
1	worker1
2	worker1
3	worker2
4	worker1
5	test1
6	worker1
7	test1
8	worker2
9	worker2
10	test1

10. Для пользователя test2 запретить доступ к одному из подключённых USB-устройств и проверить возможность его использования.

11. Для директории .\publisher включить контроль целостности с блокировкой системы при изменении файлов, задав проверку в реальном времени.

12. От имени пользователя, имеющего доступ к .\publisher, произвести изменение одного из файлов данного каталога.

13. Разблокируйте систему. Обновите запись контроля целостности, удалив предыдущую, для новой версии данного файла со следующими параметрами: обнаружение и протоколирование изменений, контроль целостности в реальном времени.

14. Отобразите события аудита для соответствующих пользователей из заданий 8, 9, 10, 12.

Контрольные вопросы

1. Возможности по настройке параметров безопасности паролей.
2. Возможности по настройке параметров входа пользователей.
3. Подсистема дискреционного разграничения доступа.
4. Настройка разграничения доступа к устройствам.
5. Контроль целостности.

Лабораторная работа № 3

Тема: Механизм замкнутой программной среды в «Secret Net LSP 1.12».

Цель работы. Изучить принципы работы механизма замкнутой программной среды в СЗИ «Secret Net LSP».

Теоретическая часть

Замкнутая программная среда

Данная подсистема позволяет ограничить использование ПО на компьютере. Это даёт возможность настроить доступ только к тем программам, которые требуются пользователям. Для этого отдельному пользователю составляется список ресурсов, включающий разрешённые для запуска программы, файлы, библиотеки, скрипты. Другие сценарии работы с компьютером запрещаются.

ЗПС работает в двух режимах: мягком и жестком. Первый предназначен для настройки механизма на основе правил, в том числе тех, которые формируются путём анализа событий журнала аудита. Второй является основным режимом. Мягкий режим позволяет собрать информацию об ошибках в конфигурации ЗПС, чтобы обеспечить корректную работу механизма при работе в жёстком режиме.

В рамках настройки и управления работой механизма замкнутой программной среды администратор выполняет следующие функции:

- управляет режимом работы механизма;
- формирует белый список пользователей и групп;
- определяет список исключений для ресурсов;
- настраивает правила контроля;
- настраивает регистрацию событий;
- проводит контроль исполняемых файлов;
- проводит аудит событий.

Общий порядок настройки

Настройка механизма замкнутой программной среды выполняется в следующем порядке:

1. Установка мягкого режима работы механизма.
2. Проведение аудита ЗПС.
3. Формирование белых списков субъектов.
4. Определение списка исключений для ресурсов.
5. Формирование и настройка правил ЗПС.
6. Настройка регистрации событий ЗПС.
7. Установка жесткого режима работы механизма.

Настройка механизма ЗПС

Для общей настройки механизма ЗПС используется плагин aec утилиты snpolctl. В плагине используется одноимённая политика, которая содержит следующие параметры (значения параметров следующие: 0 – выключено; 1 – включено):

- state – состояние;
- mode – режим работы;
- log_perm_exec – регистрация исполнения файлов;
- log_deny_exec – регистрация запрета исполнения файлов;
- log_perm_openlib – регистрация загрузки библиотек;
- log_deny_openlib – регистрация запрета загрузки библиотек;
- log_perm_openfile – регистрация открытия файлов;
- log_deny_openfile – регистрация запрета открытия файлов.

Белый список пользователей и групп

Добавление пользователя в белый список производится следующей командой:

snaecctl add -u <имя пользователя>

Аналогичная команда для группы:

snaecctl add -g <имя группы>

Проверка наличия пользователя или группы в белом списке выполняется следующей командой:

snaecctl view -U -G

В окне эмулятора терминала появится белый список пользователей.

Для удаления пользователя из белого списка:

1. Запустите программу эмулятора терминала.

2. Удалите пользователя из белого списка. Для этого выполните команду:

snaecctl rm -u <имя пользователя>

В окне эмулятора терминала появится сообщение об удалении из белого списка указанного пользователя. Для удаления нескольких пользователей необходимо перечислить их, разделяя пробелом:

snaecctl rm -u <имя пользователя1> <имя пользователя2>

3. Проверьте отсутствие пользователя в белом списке. Для этого выполните команду:

snaecctl view -U

В окне эмулятора терминала появится белый список пользователей.

Список исключений для ресурсов

Список исключений включает в себя ресурсы, для которых не осуществляется контроль ЗПС.

Для добавления ресурса в список исключений:

1. Выполните команду:

snaecctl add -r <путь к ресурсу>

В результате выполнения команды появится сообщение о добавлении в список исключений указанного ресурса. Для добавления нескольких ресурсов необходимо перечислить их, разделяя пробелом:

snaecctl add -r <путь к ресурсу1> <путь к ресурсу2>

2. Проверьте наличие ресурса в списке исключений. Для этого выполните команду:

snaecctl view -R

В окне эмулятора терминала появится список исключений ресурсов.

Для удаления ресурса из списка исключений:

1. Выполните команду:

snaecctl rm -r <путь к ресурсу>

В результате выполнения команды появится сообщение об удалении из списка исключений указанного ресурса. Для удаления нескольких ресурсов необходимо перечислить их, разделяя пробелом:

snaecctl rm -r <путь к ресурсу1> <путь к ресурсу2>

2. Проверьте отсутствие ресурса в списке исключений. Для этого выполните команду:

snaecctl view -R

В окне эмулятора терминала появится список исключений ресурсов.

Правила ЗПС

Правила ЗПС обеспечивают разграничение доступа пользователей к ресурсам. Элементы правила ЗПС перечислены в таблице 7.

Таблица 7. Элементы правила ЗПС

Элемент	Описание
Имя	Уникальный идентификатор правила
Режим	Может быть установлен следующий режим правила: - Standart – стандартный режим, который контролирует только открытие библиотек. Регистрирует события запуска и запрета запуска программ и библиотек; - Extended – строгий режим, который контролирует открытие всех файлов. Рекомендуется устанавливать для контроля исполнения скриптов. Регистрирует все события

Окончание таблицы 7

Элемент	Описание
Статус	Может быть установлен следующий статус правила: - True – правило включено; - False – правило отключено
Список пользователей и групп	Пользователи и группы, которым разрешается использование указанного списка ресурсов
Список ресурсов	Список файлов, библиотек и скриптов, разрешенных для запуска пользователем. При добавлении ресурса в правило выполняется его контроль целостности

Порядок настройки правил следующий:

- создание/обновление правила;
- добавление или обновление списка пользователей и групп;
- добавление ресурсов в правило;
- настройка режима и статуса правила;
- расчет контрольных сумм для ресурсов, указанных в правиле;
- экспорт ресурсов правила в файл;
- просмотр правила.

Добавление, переименование и удаление правил

Для добавления правила:

1. Выполните команду:

snaecctl add -n <имя правила>

В окне эмулятора терминала появится сообщение о добавлении указанного правила. По умолчанию правило будет добавлено со статусом «True» и режимом «Standart». Создается пустой список ресурсов, разрешенный для всех пользователей системы. Установка значений режима и статуса применяется только для вновь добавляемых правил. На другие правила, созданные ранее, данные изменения не распространяются.

2. Проверьте наличие добавленного правила. Для этого выполните команду:

snaecctl view -n <имя правила>

В окне эмулятора терминала появится содержимое указанного правила.

Для переименования правила:

1. Выполните команду:

snaecctl rename -n <старое имя правила> -N <новое имя правила>

В окне эмулятора терминала появится сообщение о переименовании указанного правила.

2. Для проверки успешного переименования правила выполните команду:

snaecctl view -n <новое имя правила>

В окне эмулятора терминала появится содержимое указанного правила.

Для удаления правила:

1. Выполните команду:

snaecctl rm -n <имя правила>

В окне эмулятора терминала появится запрос на подтверждение удаления указанного правила.

Удаление правила происходит безвозвратно, поэтому всегда происходит запрос подтверждения операции.

2. Подтвердите запрос. Для этого введите:

yes

В окне эмулятора терминала появится сообщение об удалении указанного правила.

3. Проверьте успешность удаления правила путём выполнения следующей команды:

snaecctl view -n <имя правила>

В окне эмулятора терминала появится сообщение об отсутствии указанного правила.

Добавление, обновление и удаление пользователей в правиле

Перед добавлением пользователей и групп в новое правило необходимо обновить список пользователей и групп. Это требуется сделать, т. к. такие правила по умолчанию разрешены для всех пользователей.

Для добавления пользователя в правило:

1. Выполните команду:

snaecctl add -n <имя правила> -u <имя пользователя>

В окне эмулятора терминала появится сообщение о добавлении пользователя в правило.

Для добавления нескольких пользователей необходимо перечислить их, разделяя пробелом:

snaecctl add -n <имя правила> -u <имя пользователя1> <имя пользователя2>

2. Выполните проверку успешного добавления пользователя в правило следующей командой:

snaecctl view -n <имя правила>

В окне эмулятора терминала появится содержимое указанного правила.

Для обновления списка пользователей в правиле:

1. Выполните команду:

snaecctl update -n <имя правила> -u <имя пользователя>

В окне эмулятора терминала появится сообщение об обновлении пользователя в правиле. Чтобы обновить нескольких пользователей в правиле, перечислите их, разделяя пробелом:

snaecctl update -n <имя правила> -u <имя пользователя1> <имя пользователя2>

2. Проверьте обновление списка пользователей в правиле. Для этого выполните команду:

snaecctl view -n <имя правила>

В окне эмулятора терминала появится содержимое указанного правила.

Для удаления пользователя из правила:

1. Выполните команду:

snaecctl rm -n <имя правила> -u <имя пользователя>

В окне эмулятора терминала появится сообщение об удалении пользователя из правила. Удаление нескольких пользователей производится путем их перечисления, разделяя пробелами:

snaecctl rm -n <имя правила> -u <имя пользователя1> <имя пользователя2>

2. Для проверки отсутствия удалённого пользователя в правиле выполните следующую команду:

snaecctl view -n <имя правила>

В окне эмулятора терминала появится содержимое указанного правила.

Добавление, обновление и удаление списка ресурсов в правиле

Для добавления списка ресурсов в правило:

1. Выполните команду:

snaecctl add -n <имя правила> -r <путь к ресурсу>

В окне эмулятора терминала появится сообщение о добавлении ресурсов в правило. Для добавления нескольких ресурсов в правило необходимо перечислить их, разделяя пробелом:

snaecctl add -n <имя правила> -r <путь к ресурсу1> <путь к ресурсу2>

2. Проверьте наличие добавленных ресурсов в правило. Для этого выполните команду:

snaecctl view -n <имя правила>

В окне эмулятора терминала появится содержимое указанного правила.

При добавлении ресурсов в правило автоматически происходит поиск зависимых библиотек с их дальнейшим добавлением в правило. Для отключения поиска зависимостей используется ключ «-d».

Для обновления списка ресурсов в правиле:

1. Выполните команду:

snaecctl update -n <имя правила> -r <путь к ресурсу> -d -R

В окне эмулятора терминала появится сообщение об обновлении списка ресурсов в правиле. Чтобы обновить несколько ресурсов в правиле, необходимо перечислить их, разделяя пробелом:

snaecctl update -n <имя правила> -r <путь к ресурсу1> <путь к ресурсу2> -d -R

2. Для проверки успешного обновления правила выполните команду:

snaecctl view -n <имя правила>

В окне эмулятора терминала появится содержимое указанного правила.

При обновлении списка ресурсов в правиле все предыдущие ресурсы удаляются из правила, на их место устанавливаются новые.

Для удаления списка ресурсов из правила:

1. Выполните команду:

snaecctl rm -n <имя правила> -r <путь к ресурсу>

В окне эмулятора терминала появится сообщение об удалении ресурсов из правила. Чтобы удалить несколько ресурсов, перечислите их, разделяя пробелом:

snaecctl rm -n <имя правила> -r <путь к ресурсу1> <путь к ресурсу2>

2. Для проверки отсутствия удалённых ресурсов в правиле выполните команду:

snaecctl view -n <имя правила>

В окне эмулятора терминала появится содержимое указанного правила.

Обновление режима и статуса правила

Для обновления режима правила:

1. Обновите режим правила на строгий. Для этого выполните команду:

snaecctl update -n <имя правила> -X

В окне эмулятора терминала появится сообщение об обновлении режима указанного правила.

2. Выполните проверку изменения режима правила:

snaecctl view -n <имя правила>

В окне эмулятора терминала появится содержимое указанного правила.

Для обновления статуса правила:

1. Выполните команду:

snaecctl disable -n <имя правила>

В окне эмулятора терминала появится сообщение об обновлении статуса указанного правила. Чтобы обновить статус нескольких правил, необходимо перечислить их, разделяя пробелом:

snaecctl disable -n <имя правила1> <имя правила2>

2. Выполните проверку изменения статуса правила:

snaecctl view -n <имя правила>

В окне эмулятора терминала появится содержимое указанного правила.

Обновление контрольных сумм правила

Для обновления контрольных сумм правила выполните команду:

snaecctl reload -n <имя правила>

В окне эмулятора терминала появится сообщение об обновлении контрольных сумм указанного правила. Чтобы обновить контрольные суммы нескольких правил, необходимо перечислить их, разделяя пробелом:

snaecctl reload -n <имя правила1> <имя правила2>

Для обновления контрольных сумм всех правил необходимо выполнить команду без указания правил.

Практическое задание

1. Включите механизм замкнутой программной среды.

2. Настройте регистрацию событий ЗПС.

3. Настройте белый список пользователей и групп. Для этого проверьте наличие в данном списке только учётной записи администратора. Также создайте пользователя worker3 и добавьте его в белый список.

4. Добавьте новые правила (для всех созданных пользователей необходимо добавить разрешающие правила для корректной работы с системой).

5. Настройте ЗПС в соответствии с таблицей 8 (для этого удалите разрешающие правила соответствующих пользователей). Также добавьте правила аудита отказа запуска указанных программ.

Таблица 8. Настройки замкнутой программной среды

Вариант	Пользователь	Запрещен запуск
1	worker1, worker2	Libre Office Calc (либо другое приложение для работы с таблицами)
2	worker2, test2	Mozilla Firefox
3	worker2, test1	Thunderbird (либо другое почтовое приложение)
4	test1, test2	Калькулятор
5	worker1, test2	Текстовый редактор
6	worker1, test1	GIMP (либо другой графический редактор)
7	worker2, test2	VLC Media Player (либо другой видеоплеер)
8	worker2, test1	Просмотр изображений
9	worker1, worker2	GParted
10	test1, test2	Libre Office Draw

6. Выполните вход в систему от имени пользователей, которым запрещен запуск программ согласно таблице, и запустите эти программы.

7. Отобразите события аудита, возникшие в результате запуска запрещённых программ.

Контрольные вопросы

1. Механизм ЗПС в Secret Net LSP.

2. Общий порядок настройки механизма ЗПС.

3. Регистрация событий ЗПС.
4. Белый список пользователей и групп.
5. Списки исключений для ресурсов.
6. Элементы правила ЗПС.
7. Порядок настройки правил ЗПС.
8. Ресурсы в правилах ЗПС.
9. Обновление контрольных сумм правила.

Лабораторная работа № 4

Тема: Персональный межсетевой экран в «Secret Net LSP 1.12».

Цель: Изучить принципы работы и порядок настройки межсетевого экрана в СЗИ «Secret Net LSP».

Теоретическая часть

Персональный межсетевой экран представляет собой компонент СЗИ Secret Net LSP, предназначенный для защиты серверов и рабочих станций от несанкционированного доступа и разграничения сетевого доступа в информационных системах.

Ниже представлены основные функции персонального межсетевого экрана:

- фильтрация с независимым принятием решений по каждому пакету;
- фильтрация пакетов служебных протоколов, необходимых для диагностики и управления работой сетевых устройств;
- фильтрация на транспортном уровне запросов к прикладным сервисам;
- фильтрация на уровне параметров протоколов стека TCP/IP;
- фильтрация на уровне пользователей или групп пользователей;
- фильтрация на уровне параметров прикладных протоколов;
- фильтрация на уровне исполняемого файла/процесса;
- фильтрация входящих соединений с использованием данных отправителя пакетов;
- фильтрация с учетом расписания;
- оповещение пользователя при срабатывании правила.

Для выполнения процедур настройки ПМЭ используется утилита fw-localcfg.

Общий порядок настройки

Настройка персонального межсетевого экрана выполняется в следующем порядке:

1. Включение ПМЭ производится следующей командой:

systemctl start snlsp-firewall

2. Получение информации о работоспособности механизма. Выполните (для выхода необходимо нажать q):

systemctl status snlsp-firewall

3. Вывод справочной информации о применении утилиты настройки ПМЭ:

fw-localcfg --help –import

4. Настройка персонального межсетевого экрана на основе правил.

Правила персонального межсетевого экрана Secret Net LSP обеспечивают выполнение функциональности механизма. В рамках настройки работы механизма администратор, обладающий правами суперпользователя компьютера, выполняет следующие действия:

- осуществляет вывод справочной информации о применении утилиты ПМЭ;
- создает новые правила;
- изменяет существующие правила;
- удаляет существующие правила;
- импортирует настройки ПМЭ из архивного файла резервной копии;
- экспортирует правила в архивный файл резервной копии;
- осуществляет вывод информации о существующих правилах;
- проводит аудит событий ПМЭ.

Пояснение

Основные процедуры, связанные с настройкой работы ПМЭ, выполняются в режиме командной строки. При работе с правилами ПМЭ в программе

эмулятора терминала необходимо соблюдать следующую последовательность вводимых команд:

[название утилиты] [<команда>] ... [<параметр=значение>]

С помощью ПМЭ осуществляется:

- фильтрация по протоколам TCP/IPv4;
- фильтрация по командам сетевых протоколов;
- фильтрация по параметрам команд;
- фильтрация по контролю доступа к ресурсам, содержащим скрипты;
- контроль доступа к именованным файлам и общим папкам;
- контроль доступа для пользователей и групп пользователей.

5. Настройка регистрации событий ПМЭ. Пример включения регистрации событий при срабатывании правила фильтрации:

fw-localcfg --add -ac=drop --proto=tcp --msg="Drop" remote_addrs=10.1.1.4 --audit=true

Также пример отключения регистрации событий при срабатывании правил фильтрации:

fw-localcfg --modify --id=4d024ebd-e5ea-47cf-8fe4-7c4dbbcff610 --audit=false

6. Проведение аудита событий ПМЭ.

Для включения срабатывания правила:

6.1. Отредактируйте файл /opt/snlsp-firewall/etc/suricata/suricata.yaml, установив для параметра «enabled» значение «yes» в секциях «- anomaly:».

Внимание!

В файле suricata.yaml для параметра «enabled» необходимо установить значение «yes» в двух секциях «- anomaly:» для журналов eve.json и alert.json.

6.2. В файле /opt/snlsp-firewall/etc/suricata/suricata.yaml установите для параметра «drop-invalid» значение «yes» в секции «stream».

6.3. Сохраните внесенные изменения в файл и закройте его.

6.4. Выполните команду:

/opt/snlsp-firewall/bin/fwfc -i

6.5. Выполните перезапуск механизма ПМЭ. Для этого выполните команду:

systemctl restart snlsp-firewall

Фильтрация сетевого трафика

Персональный межсетевой экран осуществляет фильтрацию сетевого трафика для отправителей и получателей контролируемой информации в рамках всех операций ее передачи узлам информационной системы на сетевом, транспортном и прикладном уровнях, а также предоставляет возможность явно разрешать или запрещать информационный поток на основании правил, устанавливаемых администратором. Функциональность ПМЭ обеспечивается за счет работы модуля межсетевого экранирования. Основные возможности, реализуемые модулем в рамках фильтрации сетевого трафика, представлены ниже:

- фильтрация на сетевом уровне с независимым принятием решений по каждому пакету;
- фильтрация на транспортном уровне запросов на установление виртуальных соединений (TCP-сессий);
- фильтрация на прикладном уровне запросов к прикладным сервисам;
- фильтрация пакетов протокола (ICMP, SMB);
- фильтрация с учетом полей сетевых пакетов;
- фильтрация с учетом направления трафика и сетевого интерфейса;
- фильтрация с учетом прав доступа;
- фильтрация с учетом расписания.

Практическое задание

1. Включите ПМЭ.
2. Проверьте состояние ПМЭ.

3. Далее установите новое правило ПМЭ с помощью утилиты fw-localcfg с ключом –add.

Sudo fw-localcfg -add –action=pass -protocol=any -msg='Pass packet!'
--local_addrs=192.168.0.1-192.168.0.10

При добавлении нового правила обязателен ключ –action, он говорит о том, какое действие будет совершено с пакетом (возможны значения drop и pass), также обязателен ключ –protocol, отвечающий за протокол, на основании которого осуществляется фильтрация сетевых пакетов, и ключ -msg, который добавляет текстовое сообщение. В вышеуказанной команде добавляется правило, при котором отбрасываются все пакеты, которые приходят от IP-адреса, не входящего в диапазон.

IP-адреса получателей настраиваются с помощью команды:

Sudo fw-localcfg –add –action=drop –protocol=any –msg='Drop packet!'
--local_addrs=192.168.0.1-192.168.0.10

С помощью ключей –local_ports и –remote ports настраиваются порты отправителей и получателей сетевых пакетов. Пример:

sudo fw-localcfg –add –action=drop –protocol=any –msg='Drop packet!'
--local_ports=76-92,67,55

С помощью ключа –local_ports было настроено правило, при котором отбрасываются все пакеты, пришедшие с этих портов.

Также можно добавить правило с учётом расписания. Для этого используется ключ –schedule. Установите правило, которое работает каждый час 1 и 3 числа и в период с 12 до 13 часов 2 и 4 числа следующей командой:

sudo fw-localcfg –add –action=drop –protocol=any –msg='Drop packet!'
--local_ports=76-92,67,55 –schedule= " 1,3 + # 12-13 2,4 –"*

Контрольные вопросы

1. Для чего используется ПМЭ в Secret Net LSP?
2. По каким признакам могут создаваться правила ПМЭ?
3. Каковы три обязательных ключа при добавлении правила?
4. Регистрация событий и аудит ПМЭ.

Список используемой литературы

1. Госорганизации готовятся к переходу на новую операционную систему // Алексей Михайлов, rg.ru – Интернет-портал «Российской газеты». – Дата обращения: 06.02.2024. – URL: https://rg.ru/2024/02/06/reg - szfo/ /gosorganizacii - gotoviatsia - k - perehodu - na - novuiu - operacionnuiu-sistemu.html?ysclid=lv6lrixf3h333260067.

2. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс]: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17?ysclid=lv6n09ca6h546433104.

3. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]: https://fstec.ru/ normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21?ysclid=lgxqpq7qul562917795.

4. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: https://fstec.ru/normotvorcheskaya/akty/53 - prikazy/691 - prikaz - fstek - rossii - ot - 18-fevralya-2013-g-n-21?ysclid=lgxqpq7qul562917795.

5. Код Безопасности. Средство защиты информации Secret Net LSP. Руководство администратора. – 123 с.

6. Код Безопасности. Средство защиты информации Secret Net LSP. Комментарии к версии 1.12. – 5 с.

7. Код Безопасности. Средство защиты информации Secret Net LSP. Руководство пользователя. – 22 с.

Оглавление

Введение 3
Подготовка к лабораторным работам 5
Лабораторная работа № 1 7
Лабораторная работа № 2 18
Лабораторная работа № 3 28
Лабораторная работа № 4 40
Список используемой литературы 46

Учебное издание

Шевцов Вадим Юрьевич
Булгакова Елена Валерьевна
Кубанков Александр Николаевич

ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОС СЕМЕЙСТВА LINUX С ИСПОЛЬЗОВАНИЕМ ПО SECRET NET LSP

Учебно-методическое пособие

ISBN 978-5-9729-2223-9

Подписано в печать 28.06.2024
Формат 60×84/16. Усл. печ. л. 2,79. Печать по требованию.
Бумага офсетная. Гарнитура «Таймс».

Издательство «Инфра-Инженерия»
160011, г. Вологда, ул. Козленская, д. 63
Тел.: 8 (800) 250-66-01
E-mail: booking@infra-e.ru
https://infra-e.ru