we protect your digital worlds

ESET NOD32
для защиты сервера

Руководство по установке
и документация пользователя

Содержание

ESET NOD32 для защиты файловых серверов

REV.20080306-003

Глава 1

Введение

Поздравляем вас с приобретением ESET NOD32 для защиты файлового сервера — одной из лучших систем безопасности, работающих под управлением операционных систем Linux/BSD. Используя ультрасовременное ядро сканирования ESET, система обеспечивает непревзойденные скорость сканирования и уровень обнаружения в сочетании с минимальным использованием системных ресурсов. Благодаря этому она идеально подходит для любого сервера Linux/BSD.

В данной главе будут рассмотрены ключевые характеристики системы.

- Алгоритмы антивирусного ядра сканирования ESET обеспечивают высочайший уровень обнаружения и максимальную скорость сканирования.
- Программный пакет ESET NOD32 разработан для использования, как в однопроцессорных, так и в мультипроцессорных устройствах.
- В нем используется уникальная расширенная эвристика для обнаружения червей Win32 и бэкдоров.
- Встроенные архиваторы распаковывают заархивированные объекты без использования сторонних программ.
- Архитектура системы основана на использовании демона (резидентной программы), к которому отправляются все запросы на сканирование, что приводит к увеличению скорости и эффективности работы антивирусного продукта.
- Все исполняемые демоны (за исключением esets_dac) для повышения безопасности выполняются под учетной записью непривилегированного пользователя.
- Система позволяет выполнять избирательную настройку как для индивидуальных пользователей, так и для пользователей уровня клиент-сервер.
- Для получения информации о работе системы и угрозах могут быть настроены шесть уровней ведения журналов.
- Настройка, администрирование и управление лицензиями может выполняться при помощи простого и удобного веб-интерфейса.
- В системе присутствует ESET Remote Administration для администрирования крупных компьютерных сетей.
- Для установки ESET NOD32 не требуются внешние программы или библиотеки, за исключением LIBC.
- Система может отсылать предупреждение о проникновении любому лицу, в зависимости от настроек.

Для эффективной работы ESET NOD32 требуется всего 16 МБ пространства на жестком диске и 32 МБ оперативной памяти. Эффективная работа обеспечивается под управлением ядра Linux версий 2.2.x, 2.4.x и 2.6.x, а также под управлением ядра операционной системы FreeBSD версий 5.x, 6.x.

На всех серверах, от маломощных небольших офисных систем до ISP-серверов корпоративного класса с тысячами пользователей, система обеспечивает производительность и масштабируемость, присущие решениям на ,базе UNIX, а также непревзойденную безопасность продуктов ESET.

Глава 2

Терминология и сокращения

В этой главе рассматриваются термины и сокращения, используемые в настоящей документации. Обратите внимание, что в этой документации (только для PDF-формата) полужирным шрифтом выделены названия компонентов продукта, а в данной главе таким образом выделяются также новые термины и сокращения. Также обратите внимание, что термины и сокращения, определенные в этой главе, будут выделяться и в других главах данной документации (только в PDF-формате).

ESETS

ESET Security является общей аббревиатурой для всех продуктов обеспечения безопасности, разработанных компанией ESETдля ОС Linux (и, соответственно, для ОС BSD). Также это название (или часть названия) программного пакета, включающего соответствующие продукты.

RSR

Сокращение для RedHat/Novell(SuSE) Ready. Обратите внимание, что мы поддерживаем оба варианта продукта: RedHat Ready и Novell(SuSE) Ready. Отличие от «стандартной» версии Linux заключается в том, что пакет RSR соответствует критериям, представленным в документе FHS (стандарт иерархии файловой системы (File-system Hierarchy Standard), который определяется как часть базы стандартов Linux) — документе, который требуется для сертификации RedHat Ready и Novell(SuSE) Ready. Это означает, к примеру, что пакет *RSR* устанавливается как приложение-надстройка, то есть по умолчанию предлагается путь установки /opt/eset/esets.

Демон ESETS

Основной демон системы управления и сканирования *ESETS* — **esets_daemon**.

Базовый каталог ESETS

Каталог, в котором хранятся загружаемые модули *ESETS*, в том числе, например, база данных вирусных сигнатур. Далее в документации для этого каталога будет использоваться сокращение ***@BASEDIR@***. Путь каталога:

```
Linux: /var/lib/esets
Linux RSR: /var/opt/eset/esets/lib
BSD: /var/lib/esets
```

Каталог настроек ESETS

Каталог, в котором хранятся все файлы, связанные с настройками ESET NOD32.
Далее в документации для этого каталога будет использоваться сокращение ***@ETCDIR@***.
Путь каталога:

```
Linux: /etc/esets
Linux RSR: /etc/opt/eset/esets
BSD: /usr/local/etc/esets
```

Файл конфигурации ESETS

Основной файл конфигурации ESET NOD32. Полный путь к файлу:

```
@ETCDIR@/esets.cfg
```

Каталог бинарных файлов ESETS

Каталог, в котором хранятся бинарные файлы, относящиеся к ESET NOD32. Далее в документации для этого каталога будет использоваться сокращение ***@BINDIR@***. Путь каталога:

```
Linux: /usr/bin
Linux RSR: /opt/eset/esets/bin
BSD: /usr/local/bin
```

Каталог системных ,бинарных файлов ESETS

Каталог, в котором хранятся системные бинарные файлы, относящиеся к ESET NOD32. Далее в документации для этого каталога будет использоваться сокращение ***@SBINDIR@***. Путь каталога:

```
Linux: /usr/sbin
Linux RSR: /opt/eset/esets/sbin
BSD: /usr/local/sbin
```

Каталог объектных файлов ESETS

Каталог, в котором хранятся объектные файлы и библиотеки, относящиеся к ESET Security. Далее в документации для этого каталога будет использоваться сокращение ***@LIBDIR@***. Путь каталога:

```
Linux: /usr/lib/esets
Linux RSR: /opt/eset/esets/lib
BSD: /usr/local/lib/esets
```

Глава 3

Установка

Данный продукт распространяется в виде бинарного файла:

```
esets.i386.ext.bin
```

где ext представляет собой суффикс, зависящий от дистрибутива операционной системы Linux или BSD, то есть deb для Debian, rpm для RedHat и SuSE, tgz для других дистрибутивов ОС Linux, fbs5.tgz для FreeBSD 5.xx и fbs6.tgz для FreeBSD 6.xx.

Обратите внимание, что формат бинарного файла для Linux *RSR* выглядит следующим образом:

```
esets-rsr.i386.rpm.bin
```

Для установки или обновления продукта используйте оператор:

```
sh ./esets.i386.ext.bin
```

Соответственно для версии продукта Linux RSR используйте оператор:

```
sh ./esets-rsr.i386.rpm.bin
```

В качестве ответа выводится приглашение о принятии условий лицензионного соглашения для данного продукта. После подтверждения принятия условий лицензионного соглашения установочный пакет сохраняется в текущий рабочий каталог и на терминал выводится информация, относящаяся к установке, удалению или обновлению программного обеспечения.

Установив пакет программ и запустив основной сервис *ESETS*, вы можете проверить работу системы, используя в операционной системе LINUX следующую команду:

```
ps -C esets_daemon
```

Для операционной системы BSD используется похожая команда:

```
ps -ax esets_daemon | grep esets_daemon
```

В результате выводится следующее (или сходное с ним) сообщение:

```
PID TTY    TIME CMD
2226 ?     00:00:00 esets_daemon
2229 ?     00:00:00 esets_daemon
```

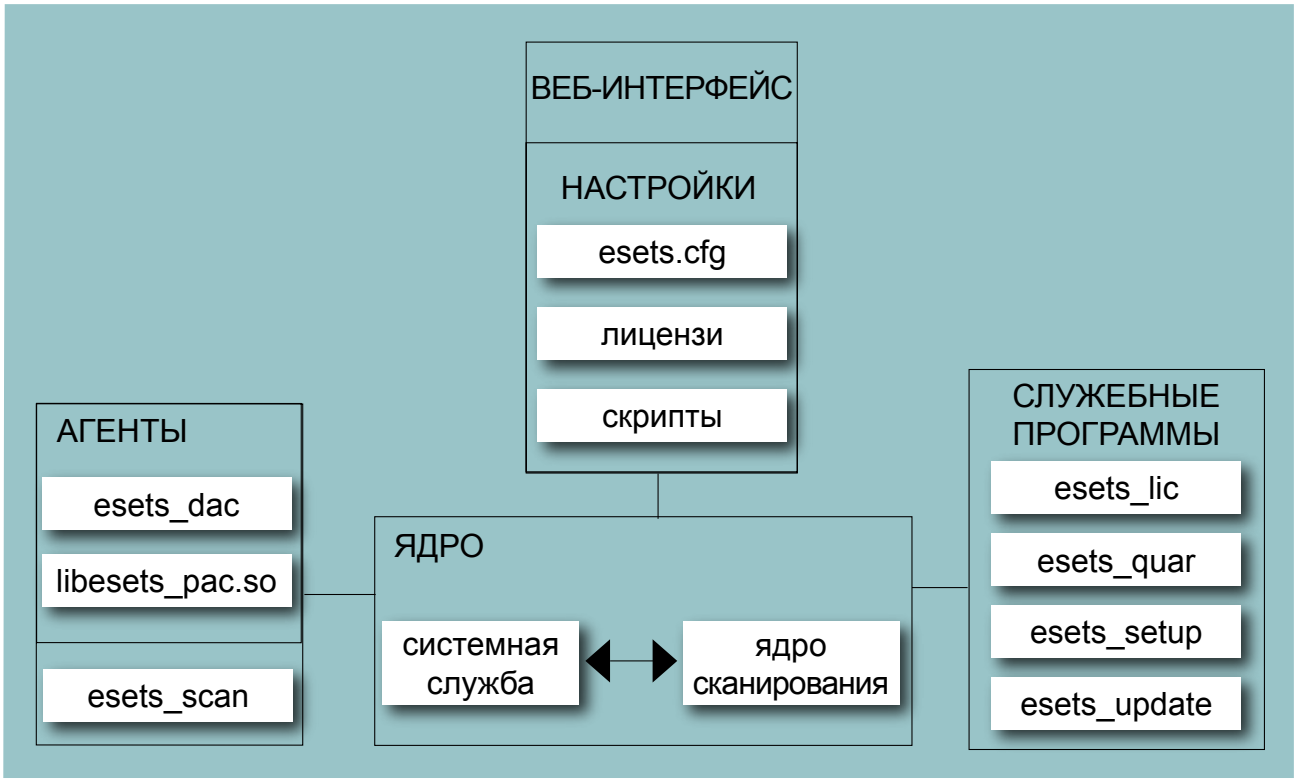
где должны быть представлены как минимум два процесса *демона ESETS*, выполняющиеся в фоновом режиме. Один из этих процессов – так называемый диспетчер процессов и потоков системы. Другой – процесс сканирования *ESETS*.

Глава 4

Структура продукта

После успешной установки пакета продукта следует ознакомиться с его содержимым.

Рис. 4–1. Структура ESET NOD32 для защиты сервера



Структура программного пакета ESET NOD32 для защиты файлового сервера показана на рисунке 4–1. Система состоит из следующих компонентов.

ЯДРО

Ядро ESET ESET NOD32 для защиты файлового сервера включает демон ESETS – esets_daemon. Этот демон использует библиотеку ESETS API libesets.so и загружаемые модули ESETS em00X_xx.dat для обеспечения основных системных задач: сканирования, агентских процессов демона, обслуживания системы предоставления образцов, ведения журналов, уведомлений и т. д. Для получения дополнительных сведений обратитесь к страницам руководства, посвященным esets_daemon (8).

АГЕНТЫ

Задачей модулей агента ESETS является интеграция ESETS с серверной средой Linux или BSD. Ознакомьтесь с соответствующей главой данного документа.

СЛУЖЕБНЫЕ ПРОГРАММЫ

Модули служебных программ являются особой частью системы. Они разработаны для обеспечения простого и эффективного управления системой и отвечают за выполнение соответствующих системных задач, например, за управление лицензиями, карантином, настройку и обновление системы. Ознакомьтесь с соответствующей главой данного документа.

НАСТРОЙКИ

Правильная настройка является важнейшим условием работы системы. Поэтому далее в этой главе будут описаны все соответствующие компоненты. Кроме того, настоятельно рекомендуется прочитать важные сведения о настройке ESETS на страницах руководства, посвященных esets.cfg (5).

После успешной установки продукта все относящиеся к нему компоненты настройки хранятся в каталоге настроек ESETS. Каталог содержит следующие файлы.

@ETCDIR@/esets.cfg

Это наиболее важный файл конфигурации, поскольку он обслуживает основную часть выполняемых продуктом функций. Посмотрев файл, вы заметите, что он состоит из различных параметров, распределенных по разделам. Обратите внимание, что названия разделов всегда заключены в квадратные скобки. В файле конфигурации ESETS всегда присутствует один глобальный раздел и несколько так называемых агентских. Параметры в глобальном разделе служат для определения настройки демона ESETS, а также значений по умолчанию для опций настройки ядра сканирования ESETS. Параметры в агентских разделах служат для определения опций настройки так называемых агентов, то есть модулей, используемых для перехвата различных типов потоков данных в компьютере или его окружении, а также для подготовки этих данных к сканированию. Обратите внимание, что помимо множества параметров, используемых для настройки системы, существует также набор правил, определяющих организацию файла. Для изучения этой информации обратитесь к разделам руководства, посвященным esets.cfg(5), esets_daemon(8), а также к разделам, описывающим соответствующие агенты.

@ETCDIR@/certs

Этот каталог служит для хранения сертификатов, используемых в веб-интерфейсом ESETS для аутентификации (для получения более подробной информации см. в раздел, посвященный esets_wwwi(8)).

@ETCDIR@/licens

Данный каталог используется для хранения лицензионных ключей продуктов, полученных от поставщика. Обратите внимание, что демон ESETS всегда обращается именно к этому каталогу для проверки правильности лицензионного ключа, если не переопределить его при помощи параметра license_dir в файле конфигурации ESETS.

@ETCDIR@/scripts/license_warning_script

Этот скрипт, если он включен параметром license_warn_enabled файла настройки ESETS, начнет выполняться за 30 дней до окончания срока действия лицензии и будет выполняться один раз в день. Он предназначен для отправки системному администратору по электронной почте уведомления об истечении срока лицензии.

@ETCDIR@/scripts/daemon_notification_script

Этот скрипт, если он включен параметром exec_script файла конфигурации ESETS, выполняется в случае обнаружения антивирусной системной вирусного проникновения. Он предназначен для отправки системному администратору по электронной почте уведомления о соответствующем событии.

Глава 5

Интеграция со службами файловой системы

В данной главе описан процесс настройки системы ESET NOD32 для сервера для обеспечения эффективной защиты файловых систем от вредоносных программ с помощью техник сканирования «по запросу» и «по доступу». Программный пакет ESET NOD32 для защиты файлового сервера включает в себя так называемые «сканер по запросу» **esets_scan** и «сканер по доступу» **esets_dac**. В Linux-версии продукта доступен также дополнительный метод сканирования по доступу, в котором используется предварительно загружаемый модуль библиотеки **libesets_pac.so**. Все упомянутые компоненты описаны в следующих разделах.

5.1. Сканирование по запросу

Сканирование по запросу — это сканирование, запускаемое привилегированным пользователем (обычно системным администратором) при помощи интерфейса командной строки или операционной системой в соответствии с расписанием планировщика команд. Объяснение термина «по запросу» заключается в том, что объекты файловой системы сканируются в результате запроса пользователя или системы.

Сканирование по запросу не подразумевает каких-либо специальных требований. После правильной установки пакета ESETS и при условии наличия действительной лицензии в каталоге лицензионных ключей сканирование по запросу может быть запущено в любой момент как через интерфейс командной строки, так и с помощью планировщика.

Для запуска сканирования по запросу из командной строки используется следующий синтаксис:

```
@SBINDIR@/esets_scan [option(s)] FILES
```

где FILES – список каталогов или файлов, подлежащих сканированию.

В сканере по запросу ESETS используются несколько опций командной строки. Ознакомиться с полным списком этих опций можно на страницах руководства, посвященным esets_scan(8).

5.2. Сканирование по доступу на ядре Dazuko

Сканирование по доступу вызывается предварительно определенным инициирующим доступом пользователей или операционной системы к объектам файловой системы. Это поясняет значение термина «по доступу», так как сканирование запускается при попытке обращения к выбранному объекту файловой системы.

Технология, используемая в *ESETS* при сканировании по доступу, основана на перехвате системных вызовов, которое осуществляется модулем ядра Dazuko (читается: «да-тзу-ко»). Проект Dazuko представляет собой бесплатное программное обеспечение. Оно распространяется в виде открытого исходного кода, что предоставляет пользователям возможность компилировать этот модуль для собственных ядер. Обратите внимание, что модуль ядра Dazuko не является частью продукта *ESETS* и поэтому его необходимо скомпилировать и установить в ядро до инициализации контроллера сканирования по доступу *ESETS* **esets_dac**. С другой стороны, метод Dazuko делает сканирование по доступу независимым от типа используемой файловой системы. Он также подходит для управления объектами файловой системы через сетевую файловую систему (Network File System (NFS)), Nettalk и Samba.

ВАЖНО. Прежде чем предоставлять подробные сведения, связанные с настройкой и использованием сканирования по доступу, мы считаем необходимым уточнить, что любой продукт *ESETS* для сканирования по доступу не предполагает обеспечение защиты всей файловой системы, в которой он установлен. Эти продукты разрабатывались и испытывались в первую очередь для обеспечения защиты внешних файловых систем. В остальных случаях необходимо предусмотреть исключение нескольких каталогов из списка контролируемых файлов, чтобы предотвратить возможное зависание системы. Обычно требуют исключения такие каталоги, как /dev и каталоги, используемые *ESETS*.

5.2.1. Принципы работы

Сканер по доступу esets_dac (контроллер доступа к файлам ESET на основе Dazuko) является резидентной программой, обеспечивающей непрерывный мониторинг и контроль файловой системы. Сканирование каждого объекта файловой системы выполняется в соответствии с настраиваемым событием доступа к файлам. В текущей версии поддерживаются следующие типы доступа к файлам:

события открытия

Этот тип доступа к файлам контролируется, если в строковом параметре event_mask в *файле конфигурации ESETS* (раздел [dac]) присутствует слово open. В этом случае устанавливается бит ON_OPEN маски доступа Dazuko.

события закрытия

Этот тип доступа к файлам контролируется, если в строковом параметре event_mask в *файле конфигурации ESETS* (раздел [dac]) присутствует слово close. В этом случае устанавливаются бит ON_CLOSE и бит ON_CLOSE_MODIFIED маски доступа Dazuko.

Обратите внимание, что в некоторых версиях ядра не поддерживается перехват событий ON_CLOSE. В этом случае события закрытия модулем esets_dac контролироваться не будут.

события выполнения

Этот тип доступа к файлам контролируется, если в строковом параметре event_mask в *файле конфигурации ESETS* (раздел [dac]) присутствует слово exec. В этом случае устанавливается бит ON_EXEC маски доступа Dazuko.

При помощи этого механизма esets_ daemon сканирует все открытые, закрытые и выполненные обычные файлы на наличие вирусов. В зависимости от результата этого сканирования, доступ к файлам будет запрещен или разрешен.

5.2.2. Установка и настройка

Как уже указывалось, так называемый модуль ядра Dazuko должен быть скомпилирован и установлен в запущенном ядре до любой инициализации esets_dac. Сведения о компиляции и установке Dazuko см. по адресу *http://www.dazuko.org/howto-install.shtml*.

После установки Dazuko прочитайте и измените разделы [global] и [dac] *файла конфигурации ESETS*. Обратите внимание, что для корректной работы сканирования по доступу необходимо включить опцию настройки agent_enabled в разделе [dac] *файла конфигурации ESETS*. Кроме того, необходимо определить объекты файловой системы (каталоги и файлы), которые должны контролироваться сканером по доступу. Это можно сделать определив параметры опций настройки ctl_incl и ctl_excl в разделе [dac] *файла конфигурации ESETS*. Для повторного считывания вновь созданной конфигурации перезагрузите *демон ESETS*.

5.2.3. Рекомендации

Чтобы обеспечить загрузку модуля Dazuko до любой инициализации демона **esets_dac**, необходимо выполнить следующие действия.

Поместите копию модуля Dazuko в какой-либо из каталогов, расположенных в каталоге, зарезервированном для модулей ядра

```
/lib/modules
```

или

```
/modules
```

Используйте служебные программы ядра depmod и modprobe (для операционной системы BSD, соответственно, kldconfig и kldload) для обработки зависимостей и правильной загрузки вновь добавленного модуля Dazuko. Вставьте следующую строку в скрип инициализации **esets_daemon** (/etc/init.d/esets_daemon) перед оператором инициализации демона.

```
/sbin/modprobe dazuko
```

Обратите внимание, что для операционной системы BSD этому соответствует строка

```
/sbin/kldconfig dazuko
```

которую следует вставить в скрипт /usr/local/etc/rc.d/esets_daemon.sh.

ВАЖНО. Очень важно, чтобы описанные выше отдельные шаги выполнялись точно в такой же последовательности, в которой они здесь перечислены. Причина заключается в том, что если модуль ядра не будет находиться в каталоге модулей ядра, служебная программа modprobe (в операционной системе BSD, соответственно, kldload) не сможет обработать загрузку модуля, что может привести к зависанию системы.

5.3. Сканирование по доступу с использованием предварительно загружаемой библиотеки LIBC

В предыдущих разделах описана интеграция системы сканирования по доступу на основе Dazuko со службами файловой системы Linux/BSD. Теперь следует отметить, что технология с использованием Dazuko, может оказаться нежелательной для системных администраторов ОС Linux, обслуживающих критические системы, если для имеющегося ядра не существует подходящего исходного кода и/или файла конфигурации, а также если ядро имеет единую,а не модульную структуру. В этом случае на помощь приходит другая технология сканирования по доступу, основанная на предварительной загрузке библиотеки LIBC.

Обратите внимание, что данный раздел предназначен только для пользователей операционной системы Linux. В этом разделе содержатся сведения о работе, установке и настройке сканирования по доступу, использующего предварительно загружаемую библиотеку **libesets_pac.so**.

5.3.1. Принципы работы

Сканер по доступу libesets_pac.so (входящий в ESETS контроллер доступа к файлам на основе предварительно загружаемой библиотеки) является библиотекой общих объектов, используемой в качестве предварительно загружаемой библиотеки LIBC, и может становиться функциональным при запуске системы. Благодаря этому он подходит для серверов файловой системы, использующих вызовы LIBC, таких как ftp-сервер, сервер Samba и т. д. Сканирование каждого объекта файловой системы выполняется в соответствии с настраиваемым событием доступа к файлу. В текущей версии поддерживаются следующие типы доступа к файлам:

события открытия

Этот тип доступа к файлам контролируется, если в строковом параметре event_mask в *файле конфигурации ESETS* (раздел [pac]) присутствует слово open. В этом случае перехватываются все функции дескриптора файлов и открытия потока FILE в LIBC.

события закрытия

Этот тип доступа к файлам контролируется, если в строковом параметре event_mask в *файле конфигурации ESETS* (раздел [pac]) присутствует слово close. В этом случае перехватываются все функции дескриптора файлов и закрытия потока FILE в LIBC.

события выполнения

Этот тип доступа к файлам контролируется, если в строковом параметре event_mask в *файле конфигурации ESETS* (раздел [pac]) присутствует слово exec. В этом случае перехватываются все функции выполнения в LIBC.

При помощи этого механизма основной демон ESETS сканирует все открытые, закрытые и выполненные обычные файлы на наличие вирусов. В зависимости от результата этого сканирования, доступ к файлам будет запрещен или разрешен.

5.3.2. Установка и настройка

Установка **libesets_pac.so** выполняется при помощи стандартного механизма установки предварительно загружаемых библиотек. Необходимо только определить переменную среды LD_PRELOAD и полный путь к библиотеке l**ibesets_pac.so**. Для получения дополнительных сведений обратитесь к страницам руководства, посвященным ld.so(8).

ВАЖНО. Необходимо отметить, что переменная среды LD_PRELOAD должна быть определена только для тех процессов демона сетевых серверов (ftp, samba и т. д.), которые требуется контролировать при помощи сканирования по доступу. Обычно предварительная загрузка вызовов LIBC во все процессы операционной системы не рекомендуется, так как это может значительно снизить производительность системы или даже привести к ее зависанию. В этой связи не должны применяться механизмы, использующие файл конфигурации etc/ld.so.preload, а также выполняющие глобальный экспорт переменной среды LD_PRELOAD. Эти механизмы будут переопределять все соответствующие вызовы LIBC во всей системе, что может привести к зависанию системы во время инициализации.

Таким образом, для перехвата только необходимых вызовов доступа к файлам, относящихся только к объектам в выбранной области файловой системы, необходимо переопределить исполняемый оператор соответствующего сервера сетевой файловой системы при помощи следующей строки:

```
LD_PRELOAD=/path/to/libesets_pac.so COMMAND COMMAND-ARGUMENTS
```

где COMMAND COMMAND-ARGUMENTS является исходным исполнимым оператором.

Прочитайте и измените разделы [global] и [pac] *файла конфигурации ESETS*. Обратите внимание, что для правильной работы сканирования по доступу необходимо определить объекты файловой системы (каталоги и файлы), которые должны контролироваться предварительно загружаемой библиотекой. Это можно сделать определив параметры опций настройки ctl_incl и ctl_excl в разделе [pac] файла конфигурации. Для повторного считывания вновь созданной конфигурации перезагрузите *демон ESETS*.

5.3.3. Рекомендации

Чтобы обеспечить работу сканирования по доступу сразу после запуска сервера сетевой файловой системы, желательно определить переменную среды LD_PRELOAD непосредственно в скрипте инициализации соответствующего сетевого файлового сервера.

ПРИМЕР. Представим, что нам необходим сканер по доступу, перехватывающий все события обращения к файловой системе сразу после запуска сервера Samba. В этом случае в скрипте инициализации, относящемся к демону Samba (/etc/init.d/smb), следует заменить оператор

```
daemon /usr/sbin/smbd $SMBDOPTIONS
```

отвечающий за инициализацию демона smbd, следующей строкой

```
LD_PRELOAD=/path/to/libesets_pac.so daemon /usr/sbin/smbd $SMBD OPTIONS
```

Таким образом, выбранные объекты файловой системы, контролируемые со стороны Samba, будут проверяться сразу после инициализации Samba, то есть во время запуска системы.

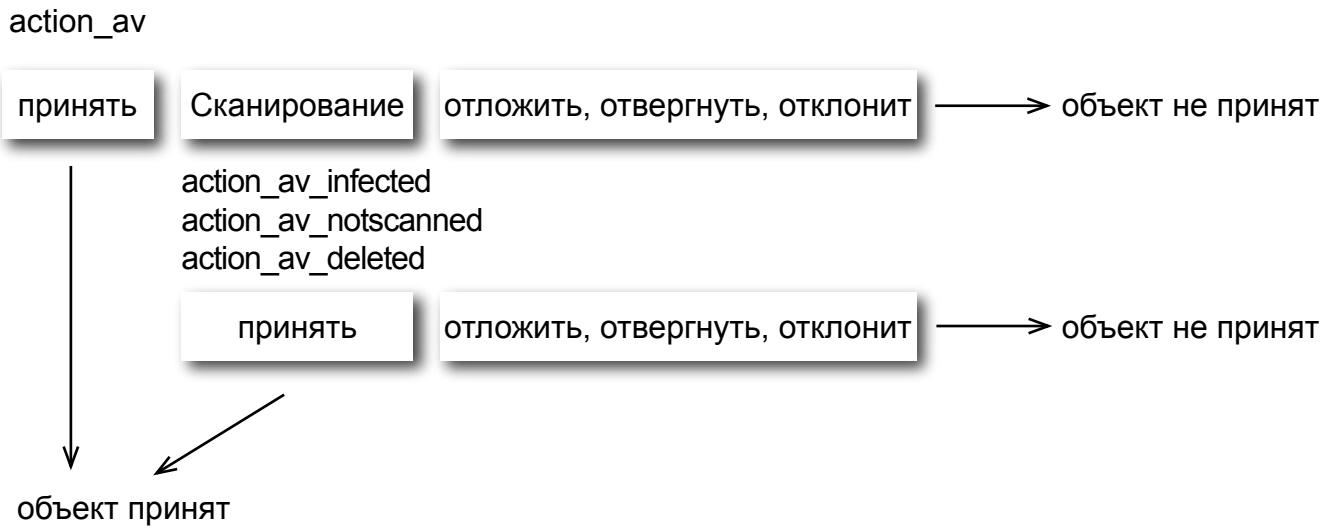
Глава 6

Основные механизмы ESET NOD32 для защиты сервера

6.1. Политика обработки объектов

Политика обработки объектов (см. рис. 6–1) – это механизм, обеспечивающий обработку просканированных объектов в соответствии с их статусом сканирования. Механизм основан на так называемых опциях настройки действий **action_av**, **action_av_infected**, **action_av_notscanned**, action_av_deleted. Для получения более подробной информации по этим опциям обратитесь к разделу руководства, посвященному esets.cfg(5).

Рис. 6–1. Схема механизма политик обработки объектов



Каждый обрабатываемый объект вначале рассматривается с учетом настройки опции конфигурации action_av. Если для опции установлено значение «принять» (accept) (соответственно, «отложить» (defer), «отвергнуть» (discard) , «отклонить» (reject)), объект будет принят (соответственно, отложен, отвергнут, отклонен). Если для опции установлено значение «сканировать» (scan), объект будет просканирован на наличие вирусов (и, соответственно, очищен, если это требуется в соответствии с опцией настройки av_clean_mode). Для оценки дальнейшей обработки объекта будет учитываться набор опций настройки действий action_av_infected, action_av_notscanned и action_av_deleted. Если в результате применения трех представленных выше опций действий было выполнено действие «принять», обработанный объект будет принят. В противном случае объект блокируется.

6.2. Настройки пользователя

В продукте используется механизм настроек пользователя, который предоставляет администратору более широкие возможности настройки. Он позволяет выборочно определять параметры антивирусного сканирования *ESETS* в отношении пользователя, который обращается к объектам файловой системы.

Более подробное описание этих возможностей см. в разделе руководства, посвященном esets.cfg(5), а также в указанных там разделах. Поэтому здесь будет приведен лишь краткий пример настройки пользователя.

Предположим, esets_dac используется для контроля событий доступа ON_OPEN и ON_EXEC в отношении внешнего диска, подключенного в каталоге /data. Модуль управляется разделом настройки [dac] в *файле конфигурации ESETS*. Раздел выглядит следующим образом.

```
[dac]
agent_enabled = yes
event_mask = 5
ctl_incl = ”/home”
action_av = ”scan”
```

Чтобы указать индивидуальные настройки параметров, необходимо определить параметр user_config и путь к особому файлу конфигурации, в котором хранятся эти настройки. В следующем примере создается ссылка на файл специальных настроек esets_dac_spec.cfg, расположенный в *каталоге настроек ESETS*.

```
[dac]
agent_enabled = yes
event_mask = 5
ctl_incl = ”/home”
action_av = ”scan”
user_config = ”esets_dac_spec.cfg”
```

После создания в разделе [dac] ссылки на файл специальных настроек необходимо создать этот файл в каталоге настроек ESETS и прописать в нем соответствующие индивидуальные настройки.

```
[username]
action_av = ”reject”
```

Обратите внимание, что название заголовка особого раздела содержит сведения идентификации пользователя, для которого созданы индивидуальные настройки. В теле раздела содержатся индивидуальные параметры, указанные для соответствующей идентификационной записи. Таким образом, данная особая настройка позволит обрабатывать запросы всех пользователей, которые пытаются получить доступ к файловой системе. То есть все объекты файловой системы, доступ к которым получают пользователи, будут сканироваться на наличие вирусов. При этом попытки доступа пользователя username будут отклоняться, то есть блокироваться, в любом случае.

6.3. Система предоставления образцов

Система предоставления образцов – это интеллектуальная технология ThreatSense.NET, которая обеспечивает перехват зараженных объектов, обнаруженных методом расширенной эвристики, и доставку этих объектов на сервер системы предоставления образцов. Все образцы вирусов, отобранные системой предоставления образцов, будут обработаны сотрудниками вирусной лаборатории компании ESET и затем при необходимости добавлены в базу данных вирусов ESET.

ПРИМЕЧАНИЕ. В СООТВЕТСТВИИ С УСЛОВИЯМИ НАШЕГО ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ, ЗАПУСКАЯ СИСТЕМУ ПРЕДОСТАВЛЕНИЯ ОБРАЗЦОВ, ВЫ ДАЕТЕ РАЗРЕШЕНИЕ КОМПЬЮТЕРУ ИЛИ ПЛАТФОРМЕ, НА КОТОРОЙ УСТАНОВЛЕН ДЕМОН ESETS_DAEMON, СОБИРАТЬ ДАННЫЕ (КОТОРЫЕ МОГУТ ВКЛЮЧАТЬ ЛИЧНЫЕ СВЕДЕНИЯ О ВАС И ПОЛЬЗОВАТЕЛЯХ ДАННОГО КОМПЬЮТЕРА) И ОБРАЗЦЫ ВНОВЬ ОБНАРУЖЕННЫХ ВИРУСОВ ИЛИ ДРУГИХ УГРОЗ И ОТПРАВЛЯТЬ ИХ В НАШУ ВИРУСНУЮ ЛАБОРАТОРИЮ. ПО УМОЛЧАНИЮ ЭТА ФУНКЦИЯ ОТКЛЮЧЕНА. ЭТА ИНФОРМАЦИЯ И ДАННЫЕ БУДУТ ИСПОЛЬЗОВАНЫ НАМИ ТОЛЬКО ДЛЯ ИЗУЧЕНИЯ УГРОЗ, И МЫ ПРИМЕМ ВСЕ ЦЕЛЕСООБРАЗНЫЕ МЕРЫ ПО СОХРАНЕНИЮ КОНФИДЕЦИАЛЬНОСТИ ДАННОЙ ИНФОРМАЦИИ.

Для включения системы выдачи образцов требуется подключить её кэш. Для этого следует включить опцию настройки samples_enabled в разделе [global] *файла конфигурации ESETS*. Чтобы включить процесс предоставления образцов на серверы вирусной лаборатории ESET, необходимо также включить параметр samples_send_enabled в том же разделе.

Пользователь может принять решение о предоставлении сотрудникам вирусной лаборатории ESET дополнительных сведений. Для этого используются опция samples_provider_mail или samples_provider_country. Эта информация помогает получению представления о том, какие угрозы распространяются через Интернет.

Для получения более подробной информации о системе предоставления образцов обратитесь к разделу руководства, посвященному esets_daemon(8).

6.4. Веб-интерфейс

Веб-интерфейс обеспечивает удобство настройки, администрирования и управления лицензиями ESETS.

Этот модуль является отдельной программой-агентом и должен быть активирован явным образом. Для быстрого запуска установите все следующие опции в *файле конфигурации ESETS* и перезапустите *демон ESETS*:

```
[wwwi]
agent_enabled = yes
listen_addr = адрес
listen_port = порт
username = имя
password = пароль
```

(введите вместо всех четырех значений ваши данные) и введите в адресной строке браузера https://address:port (обратите внимание: *https*), а затем выполните вход со сведениями учетной записи name/pass (имя/пароль). Основные инструкции по использованию см. на странице справки. Для получения более подробной технической информации о **esets_wwwi** обратитесь к разделу руководства, посвященному esets_wwwi(1).

6.5. Удаленное администрирование

В ESETS используется ESET Remote Administration для обеспечения удаленного управления в компьютерных сетях. Более подробные сведения см. в руководстве по ESET Remote Administrator.

Клиент ESETS Remote Administration является частью основного демона ESETS. Для выполнения основной настройки укажите адрес сервера ERA в параметре racl_server_addr (и racl_password, если необходимо) в разделе [global] файла конфигурации ESETS. Все переменные клиента RA см. на страницах руководства, посвященных esets_daemon(8).

Клиент Unix ESETS RA обладает следующей функциональностью:

- вход на сервер ERA и предоставление системных сведений, данных о конфигурации, состоянии и характеристиках защиты
- конфигурацию можно просмотреть и изменить при помощи редактора конфигурации ESET (ESET Configuration Editor), также применить при помощи задачи «Конфигурирование»
- выполнение задач «Сканирование по запросу» (On-Demand Scan) и «Обновить сейчас» (Update Now) по требованию с отправкой журналов сканирования на сервер ERA
- отправка важных результатов сканирования, выполненного демоном ESETS, в журнал угроз
- отправка всех сообщений, не относящихся к отладке, в журнал событий

Следующие функции не поддерживаются:

- журнал файервола
- удаленная установка

Глава 7

Обновление системы ESET Security

7.1. Служебная программа обновления ESETS

Для обеспечения эффективности работы ESET NOD32 для защиты сервера требуется регулярное обновление базы данных вирусных сигнатур. Для этой цели разработана служебная программа esets_update (дополнительные сведения см. на страницах руководства, посвященных esets_update(8)). Чтобы запустить обновление, необходимо определить опции настройки av_update_username и av_update_password в разделе [global] файла конфигурации ESETS. Следует учесть, что при подключении к Интернету через HTTP-прокси также необходимо указать опции proxy_addr, proxy_port и при необходимости proxy_username и proxy_ password. Для запуска обновления введите команду:

```
@SBINDIR@/esets_update
```

Для обеспечения максимальной безопасности сотрудники ESET непрерывно собирают определения вирусов по всему миру. Новые образцы могут появляться в базе через очень короткие промежутки времени. Поэтому рекомендуется регулярно выполнять обновление. Обратите внимание, что демон ESETS может выполнять периодическое обновление системы, если демон запущен и в разделе [global] *файла конфигурации ESET* указана опция av_update_period.

7.2. Описание процесса обновления ESETS

Процесс обновления состоит из двух этапов. Во-первых, с исходного сервера ESET загружаются так называемые предварительно скомпилированные модули. Если в разделе [global] файла конфигурации ESETS включена опция настройки av_mirror_enabled, в каталоге будет создаваться зеркало этих модулей:

```
@BASEDIR@/mirror
```

Следует учесть, что путь к каталогу зеркала может быть переопределен при помощи опции настройки av_mirror_dir в разделе [update] файла конфигурации ESET. Таким образом, вновь созданное зеркало служит как полнофункциональный сервер загрузки модулей и может использоваться для создания подчиненных зеркал. Однако при этом требуется соблюдение нескольких условий. Во-первых, на компьютере, откуда будут загружаться модули, должен быть установлен http-сервер. Во-вторых, модули, подлежащие загрузке другими компьютерами, должны быть расположены в каталоге с путем:

```
/http-serv-base-path/eset_upd
```

где http-serv-base-path является основным путем к каталогу http-сервера, поскольку это первое расположение, где служебная программа обновления ищет модули.

Вторым этапом процесса обновления является компиляция модулей, загружаемых сканером ESET NOD32 для защиты почты, из модулей, сохраненных в локальном зеркале. Обычно создаются следующие модули загрузки ESETS: модуль загрузчика (em000.dat), модуль сканирования (em001.dat), модуль базы данных вирусных сигнатур (em002.dat), модуль поддержки архивов (em003.dat), модуль расширенной эвристики (em004.dat) и т. д. в каталоге:

```
@BASEDIR@
```

Обратите внимание, что это тот же каталог, из которого демон ESETS загружает модули. Таким образом, он может быть переопределен при помощи параметра конфигурации base_dir в разделе [global] файла конфигурации ESETS.

Глава 8

Обратная связь

Уважаемый пользователь! Данное руководство должно было предоставить достаточный объем сведений об установке, настройке и поддержке программного пакета ESET NOD32 для защиты файловых серверов. Однако написание документации никогда нельзя считать завершенным. Всегда будут обнаруживаться отдельные моменты, которые могли бы быть освещены лучше или даже не были затронуты совсем. Поэтому просим сообщать о найденных в данной документации ошибках или несоответствиях в наш центр поддержки по адресу

http://esetnod32.ru/support/

Будем рады помочь в решении любых проблем, касающихся данного продукта.

Приложение А. Лицензия PHP

Лицензия PHP, версия 3.01, (c), 1999–2006 PHP Group. Все права защищены. Распространение и использование в форме исходных кодов и бинарных файлов, с изменениями или без таковых, разрешается при условии соблюдения следующих условий.

1. Распространение исходного кода должно происходить с сохранением вышеуказанного уведомления об авторских правах, данного списка условий и приведенного ниже отказа от ответственности.

2. При распространении в форме бинарных файлов в документации и/или других материалах, предоставляемых с дистрибутивом, должны воспроизводиться вышеуказанное уведомление об авторских правах, данный список условий и приведенный ниже отказ от ответственности.

3. Название «PHP» не должно использоваться для поддержки или продвижения продуктов, созданных на основе данного программного обеспечения, без предварительного письменного разрешения. Для получения письменного разрешения обратитесь по адресу group@php.net.

4. Продукты, созданные на основе данного программного обеспечения, не могут быть названы «PHP», и «PHP» не может являться частью их наименования без предварительного письменного разрешения, которое может быть получено по адресу group@php.net. Допускается указание того, что программное обеспечение работает в сочетании с PHP. В этом случае должна использоваться формулировка «Нечто для PHP» вместо названия «Нечто PHP» или «phpнечто».

5. PHP Group может публиковать обновленные и/или новые версии лицензии при необходимости. Каждой версии будет присваиваться отличительный номер. После публикации рассматриваемого здесь кода в рамках конкретной версии лицензии его использование может продолжаться в соответствии с условиями упомянутой версии. Также можно использовать рассматриваемый здесь код в соответствии с условиями любой последующей версии лицензии, опубликованной PHP Group. PHP Group обладает исключительным правом изменять условия, применимые к рассматриваемому здесь коду, созданному всоответствии с данной лицензией.

6. При распространении в любой форме должно сохраняться следующее уведомление: «В данном продукте содержится программное обеспечение PHP, свободно распространяемое и доступное по адресу http://www.php.net/software/».

ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРЕДОСТАВЛЕНО ГРУППОЙ РАЗРАБОТЧИКОВ PHP «КАК ЕСТЬ». НАСТОЯЩИМ ЗАЯВЛЯЕТСЯ ОТКАЗ ОТ ЛЮБЫХ ГАРАНТИЙ, ЯВНЫХ ИЛИ СКРЫТЫХ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ) СКРЫТЫЕ ГАРАНТИИ ПРИГОДНОСТИ И АДЕКВАТНОСТИ КОНКРЕТНОЙ ЦЕЛИ. ГРУППА РАЗРАБОТЧИКОВ PHP ИЛИ ЕЕ УЧАСТНИКИ НИ В КАКОМ СЛУЧАЕ НЕ БУДУТ НЕСТИ ОТВЕТСТВЕННОСТЬ ЗА ЛЮБЫЕ ПРЯМЫЕ, КОСВЕННЫЕ, ДОПОЛНИТЕЛЬНЫЕ, ШТРАФНЫЕ ИЛИ ПОБОЧНЫЕ УБЫТКИ/УЩЕРБ (ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ) ПРИОБРЕТЕНИЕ СУРРОГАТНЫХ ТОВАРОВ И УСЛУГ, УБЫТКИ, НЕДОПОЛУЧЕНИЕ КОММЕРЧЕСКОЙ ПРИБЫЛИ, ПРЕРЫВАНИЕ КОММЕРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ, УТРАТУ КОММЕРЧЕСКИХ СВЕДЕНИЙ И ТОМУ ПОДОБНОЕ), ВОЗНИКШИЕ ПО КАКОЙ-ЛИБО ПРИЧИНЕ ИЛИ НА ОСНОВАНИИ КАКОЙ-ЛИБО ТЕОРИИ ОТВЕТСТВЕННОСТИ, КАК КОНТРАКТНОЙ, ТАК И ОБЪЕКТИВНОЙ ЛИБО ГРАЖДАНСКОЙ (ВКЛЮЧАЯ ХАЛАТНОСТЬ ИЛИ ИНОЕ), ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ЛЮБЫМ СПОСОБОМ, ДАЖЕ ЕСЛИ БЫЛО ИЗВЕСТНО ЛИБО ДОЛЖНО БЫЛО БЫТЬ ИЗВЕСТНО О ВОЗМОЖНОСТИ ТАКИХ УБЫТКОВ/УЩЕРБА.