Руководство по Безопасности

В этом руководстве объясняются основные концепции безопасности в SUSE Linux Enterprise Server. Оно охватывает обширную документацию о таких механизмах аутентификации, доступных в Linux, как NIS или LDAP. Оно также обращается к различным аспектам локальной безопасности вроде списков контроля доступа (ACL), шифрования и обнаружения вторжений. В части, касающейся безопасности сети, вы научитесь защищать компьютеры с помощью файерволла и маскарадинга, а также настраивать виртуальные частные сети (VPN). В этом руководстве также будет показано, как использовать встроенное программное обеспечение по безопасности вроде Novell AppArmor (которое позволяет указать программе, какие именно файлы она может читать, записывать и выполнять) или системы аудита, надежно собирающей сведения о любых событиях, относящихся к вопросам безопасности.

Многие разделы этого руководства содержат ссылки на дополнительную документацию. Они включают в себя как документацию, доступную в системе, так и находящуюся в Интернете.

Перевод: Hrafn (http://hrafn.me)

1.0 Безопасность и Конфиденциальность

Одной из основных характеристик систем Linux или Unix является возможность управлять несколькими пользователя одновременно (многопользовательская) и позволять этим пользователям выполнять несколько задач (многозадачная) на одной и той же машине одновременно. Кроме того, операционная система работает в сети совершенно прозрачно. Часто пользователи даже не знают, предоставляются ли данные и приложения, которые они используют, локальной машиной или через сеть.

При использовании многопользовательских возможностей данные разных пользователей должны храниться раздельно. Необходимо гарантировать их безопасность и конфиденциальность. Безопасность данных уже давно является важной проблемой, еще с того времемени, когда компьютеры не были объединены в сети. Так и сегодня, наиболее важной задачей является обеспечение доступности данных, несмотря на потерю или повреждение носителя данных, которым, в большинстве случаев, бывает жесткий диск.

В этом разделе в первую очередь обращается внимание на проблемы конфиденциальности и способы защиты конфицендиальности пользователей, но делать упор только на этом недостаточно, потому как всесторонняя концепция безопасности всегда должна включать в себя такие процедуры как регулярно обновляемые, работоспособные и проверенные резервные копии. При отсутствии этого у вас наступит очень тяжелое время, пока вы будете пытаться вернуть свои данные — не только в случае какого-либо аппаратного дефекта, но и при возникновении подозрений, что кто-то смог получить несанкционированный доступ и нанести ущерб файлам.

1.1 Локальная и Сетевая Безопасность

Есть несколько способов получения доступа к файлам:

- личная связь с людьми, которые обладают необходимой информацией или имеют доступ к данным на компьютере
- непосредственный доступ к консоли компьютера (физический доступ)
- через последовательные линии
- используя сеть

Во всех этих случаях, до предоставления доступа к ресурсам или данным необходимо установить подлинность пользователя. Веб-сервер возможно менее ограничен в этом аспекте, но вы вряд ли хотите раскрывать ваши персональные данные другому пользователю в сети.

В указанном выше списке первый пункт — это тот случай, в котором происходит большое количество взаимодействий между людьми. Например, когда вы общаетесь с банковским служащим и вам требуется доказать, что вы именно тот человек, которому принадлежит банковский счет. Затем у вас просят подпись, PIN или пароль для доказательства, что вы — именно тот, за кого себя выдаете. В некоторых случах, есть возможность вытянуть некоторые сведения из информированного источника, просто упоминая некоторые детали и подробности и используя умные слова, чтобы получить доверие этого человека. Жертву можно убедить предоставить немного больше информации и она даже не будет знать об этом. Среди хакеров это называется **социальной инженерией**. Вы можете защититься от этого, только обучая людей разговаривать и делиться информацией совершенно осознанно.

Человек, желающий получить несанкционированный доступ к вашим данным,

также может использовать традиционный путь и попробовать добраться непосредственно к вашему оборудованию. По этой причине, машину необходимо защищать от любого вмешательства таким образом, чтобы никто не мог удалить, подменить или испортить ее компоненты. Это также относится к резервным копиям и сетевому кабелю или шнуру питания. Также необходимо обезопасить процесс загрузки, так как существует несколько известных клавиатурных комбинаций, которые могут спровоцировать странное поведение. Защитите себя от этого, установив пароли на BIOS и загрузчик.

Во многих местах все еще используются терминалы, подключенные к последовательным портам. В отличие от сетевых интерфейсов они никак не зависят от сетевого протокола для связи с хостом. Для отправки простых символов между устройствами используется простой кабель или инфракрасный порт. Кабель сам по себе — самое слабое звено в такой системе: с помощью старого принтера, подключенного к нему, легко записать все, что передается по этому кабелю. Что можно получить с помощью принтера — можно получить и другими способами, все зависит от усилий, прилагаемых при атаке.

Чтение файла локально на хосте требует немного других прав доступа, чем открытие сетевого подключения с сервером с дургого хоста. Существует различия между локальной безопасностью и сетевой безопасностью. Граница проходит в том месте, где данные должны быть помещены в пакеты для отправки в какое-либо другое место.

1.1.1 Локальная Безопасность

Локальная безопасность начинается с физического окружения в том месте, где работает компьютер. Установите машину в такое место, где безопасность обеспечивается согласно вашим ожиданиям и потребностям. Основная цель локальной безопасности — держать пользователей отдельно друг от друга таким образом, чтобы никто не мог получить чужие права или выдать себя за другого. Это основное правило, которое должно соблюдаться, но оно особенно верно для пользователя root, в руках которого находится вся власть над системой. Root может получить права любого локального пользователя без необходимости ввода пароля и читать любые хранящиеся локально файлы.

1.1.2 Пароли

На Linux-системах пароли не хранятся открытым текстом и введенная текстовая строка не просто сравнивается с сохраненным шаблоном. Если бы это делалось именно так, все учетные записи на вашей системе были бы подставлены под угрозу в случае, если кто-нибдуь смог бы получить доступ к этому файлу. Вместо этого сохраненные пароли шифруются и каждый раз, когда они вводятся, они снова шифруются, а затем две шифрованные строки уже сравниваются. Только это обеспечивает вероятность того, что пароль не может быть вычислен обратно в оригинальный текст.

Фактически это достигается с помощью специального алгоритма, который называется **trapdoor algorithm** (алгоритм с секретом), поскольку работает только в одном направлении. Злоумышленник, получивший зашифрованную строку, не может получить ваш пароль, снова применив тот же алгоритм. Вместо этого, ему придется проверить все возможные комбинации символов до тех пор, пока найденная комбинация не будет выглядеть, как ваш зашифрованный пароль. С паролем в восемь символов длиной имеется достаточно много всевозможных комбинаций для вычисления.

В 70-е все были убеждены, что этот метод более безопасный, чем другие, благодаря относительно медленной скорости использующегося алгоритма, который занимал

несколько секунд для шифрования одного пароля. В наше время, однако, персональные компьютеры стали достаточно мощными для того, чтобы производить несколько сотен тысяч или даже миллионов операций в секунду. По этой причине, шифрованные пароли не доолжны быть доступны для обычных пользователей (файл `/etc/shadow` обычные пользователи прочитать не могут). И гораздо более важно, чтобы пароли были достаточно сложны для отгадывания втом случае, если они станут доступны в результате какой-либо ошибки. Поэтому, на самом деле не очень удачный вариант «переводить» пароль "tantalize" в `"t@nt@1lz3"`.

Замена нескольких букв в слове подобными им цифрами не достаточно безопасна. Программы для взлома паролей, использующие словари для перебора, легко определяют подобные слова. Гораздо лучше составить слово, не имеющего какого-либо значения, имеющие смысл только для вас лично, например, первые буквы слов предложения или заглавия книги, например, "The Name of the Rose" Умберто Эко. Это позволяет получить следующий достаточно безопасный пароль: "TnotRbUE9". К слову, пароли вроде "beerbuddy" или "jasmine76" легко угадать любому, кто хоть немного о вас знает.

1.1.3 Процесс загрузки

Настройте систему таким образом, чтобы она не могда быть загружена с флоппи-диска или с CD, удалите приводы полностью или установите пароль на BIOS, а в BIOS настройте возможность загрузки только с жесткого диска. Обычно система Linux запускается с загрузчика, который позволяет передать дополнительные опции ядру. Чтобы воспрепятствовать этому, настройте специальные параметры загрузки, указав дополнительный пароль в `/boot/grub/menu.lst` (смотрите Section 9.0, "The Boot Loader GRUB," (↑ Administration Guide)). Это очень важно для безопасности вашей системы. Важно не только не позволять ядру работать с правами пользователя root, но требовать обязательной авторизации для получения прав root'а для изменения параметров ядра при старте системы.

1.1.4 Права на файлы

Общее правило — всегда работать с как можно наиболее ограниченными правами, необходимыми для выполнения поставленной задачи. Например, нет никакой необходимости быть пользователем root, чтобы читать электронную почту или написать письмо. Если в почтовой программе есть ошибка, эту ошибка может быть использована для атаки, и атака будет происходить с теми же правами, с которыми была запущена программа. Следование упомянутому правилу, позволит минимизировать возможные проблемы.

Права на все файлы, включенные в дистрибутив SUSE Linux Enterprise Server были тщательно отобраны. Системный администратор, который устанавливает дополнительное программное обеспечение или другие файлы, должен делать это с повышенной осторожностью, особенно, определяя права. Опытные и серьезно относящиеся к безопасности администраторы всегда используют опцию `-l` команды `ls` для получения расширенного списка файлов, что позволяет сразу определить некорректно выставленные права на файлы. Некорректные аттрибуты файла не только означают, что файлы могут быть изменены или удалены. Измененные файлы могут выполняться с правами пользователя root, или, в случае с файлами конфигурации, программы будут использовать такие файлы с правами пользователя root, что значительно увеличит возможности атакующего. Атаки, подобные этой, называют «яйца кукшки», так как программа (яйцо) выполняется (высиживается) другим пользователем (птицей), так же как кукушка обманом заставляет других птиц высиживать ее яйца.

В систему SUSE Linux Enterprise Server входят файлы разрешений, `permissions.easy`,

`permissions.secure` и `permissions.paranoid`, все в каталоге `/etc`. Назначение этих файлов — определить специальные разрешения, например, определить каталоги, запись в которые разрешена всем, или, для файлов, SUID-бит (программы с установленным setuser ID запускаются не с правами пользователя, оторый их запустил, а с правами владельца файла, чаще всего — root). Для добавления своих собственных настроек администратор может использовать файл `/etc/permissions.local`.

Для определения, какой из этих файлов используется программой конфигурации SUSE Linux Enterprise Server для установки соответствующих разрешений, выберите *Local Security* в разделе *Users and Security* в Yast. Для получения более подробной информации прочтите комментарии в файле `/etc/permissions` или обратитесь к man-странице программы `chmod` (man chmod).

1.1.5 Переполнение буфера и Ошибки Функции Форматирования Строк

Следует обратить отдельное внимание на тот случай, когда программа обрабатывает данные, которые могут или могли бы быть изменены пользователем, но об этом гораздо больше должны заботиться создатели приложения, а не обычные пользователи. Программист должен убедиться, что его приложение корректно интерпретирует данные, не записывая данные в область памяти, которая слишком мала для хранения таких данных. Также, программа должна передавать данные последовательным образом, используя интерфейсы, предназначенные для этих целей.

Переполнение буфера может произойти в том случае, если фактический размер буфера памяти не принимается во внимание при записи в этот буфер. Есть случаи, когда эти данные (как сгенерированные пользователем) используют гораздо больше пространства, чем доступно в буфере. В результате, данные записываются за пределами конца области буфера, которая, при определенных обстоятельствах, позволяет программе выполнить последовательность программ, указанную пользователем (а не программистом) вместо того, чтобы просто обработать данные пользователя. У подобных ошибок могут быть серьезные последствия, особенно, если программа выполняется со специальными привилегиями (смотрите Section 1.1.4, File Permissions).

Ошибки функции форматирования строки работают немного по-другому, но снова данные вводит пользователь, что может сбить программу с пути. В большинстве случаев, эти программные ошибки эксплуатируются программами, выполняющимися со специальными правами — программы с установленными setuid и setgid — это также означает, что вы можете защитить свои данные и систему от таких ошибок, убрав соответствующие права на выполнение у этих программ. И снова, лучший выход — применять политику использования как можно более низких привилегий (смотрите Section 1.1.4, File Permissions).

Установлено, что переполнения буфера и ошибки функции форматирвоания строки — это ошибки, связанные с обработкой данных пользователя, они выполнимы не только в том случае, елси получен доступ к локальной учетной записи. Многие из ошибок, о которых было рассказано, могут эксплуатироваться через еть. Соответственно, переполнения буфера и ошибки функции форматирования строки необходимо классифицировать в качестве относящихся как к локальной. Так и сетевой безопасности.

1.1.6 Вирусы

Вопреки тому, что некоторые люди говорят, существуют вирусы, которые запускаются на Linux. Однако, известные вирусы были выпущены их авторами в качестве **доказательства концепции**, что эта методика работает так, как и была

задумана. Ни один из вирусов пока не был найден **в живой природе**.

Вирусы не могут выжить и распространяться без хоста, на котором они живут. В этом случае, хост становится программой или важной областью хранения системы, например, главная загрузочная запись (MBR), на которую программный код вируса должен иметь права на запись. Вследствие многопользовательской природы, Linux может ограничивать права записи в определенные файлы, особенно в важные системные файлы. Поэтому, если вы обычно работает с правами пользователя root, вы увеличиваете шансы заражения системы вирусами. И напротив, при следовании принципам использования наименьших привилегий, шансы получения вируса становятся крайне призрачными.

Кроме того, никогда не запускайте программу, полученную с другого узла Интернет, который вам не известен. RPM-пакеты SUSE Linux Enterprise Server включают в себя криптографическую сигнатуру, в качестве цифровой метки, необходимую для их создания. Вирусы — это типичный признак, что администратор или пользователь недостаточно понимают концепции безопасности, этим ставя под угрозу систему, которая должна быть безопасна по своему дизайну.

Вирусы нельзя путать с червями, которые полностью относятся к миру сетей. Черви не нуждаются в основном компьютере для распространения.

1.1.7 Сетевая безопасность

Сетевая безопасность важна для защиты от атак, проходящих снаружи. Обычный процесс входа в систему, требующий имя пользователя и пароль для аутентификации, все ще относится к локальной безопасности. В исключительном случае входа через сеть необходимо различать разницу между аспектами безопасности. То, что происходит до фактической аутентификации — это сетевая безопасность, все что после — локальная.

1.1.8 X-Window System и аутентификация в X

Как уже было сказано в самом начале, прозрачность сети — одна из основных характеристик систем Unix. X, оконная система операционных систем Unix, может сделать использование этой возможности очень впечатляющим.

В случае, когда X клиентов удаленно подключается к X-серверу, последний должен защитить ресурсы, управляемые им (дисплеем) от неавторизованного доступа. Если выражаться точнее, клиентской программе должны быть даны определенные права. Эта два способа сделать это: контроль доступа на основе хота и контроль доступа на основе cookie. Первый зависит от IP-адреса хоста, на котором запущен клиент. Программа, которолирующая это, называется xhost. Xhost вводит IP-адрес настоящего клиента в крошечную базу данных X-сервера. Однако, доверять IP-адресам при аутентификации не очень безопасно. Например, если есть второй пользователь, работающий на хосте, передаст клиентскую программу, то этот пользователь также получит доступ к X-серверу — точно так же, как если бы кто-нибудь подменил IP-адрес. По этим причинам, данный способ описывается здесь не очень подробно, но вы можете узнать о нем, обратившись к `man xhost`.

В случае второго способа контроля доступом, генерируется строка символов, которая известна только X-серверу и легитимному пользователю, как некоего рода, удостоверение личности. Это «печенье» (но не как слово, относящееся к обычному печенью, а что-то вроде китайских печений судьбы, содержащих эпиграмму) сохраняется при входе в файле `.Xauthority` в домашнем каталоге пользователя и доступно для любого X-клиента, желающего использовать X-сервер для отображения окон. Файл `.Xauthority` может быть проверен пользователем с помощью инструмента `xauth`. Если случайно переименуете или удалите этот файл из домашнего каталога пользователя, вы не сможете открыть новое окно или X-

клиентов.

SSH (secure shell) может использоваться для полного шифрования сетевого подключения и прозрачного перенаправления его к X-серверу. Это также называется X forwarding. X forwarding выполняет имитацию X-сервера на стороне сервера и устанавливать переменную DISPLAY для шелла на удаленном хосте. Более подробно об этом можно прочитать в Разделе 14.0, SSH: Secure Network Operations.

ВНИМАНИЕ: Если вы не считаете хост, на котором залогинились, достаточно безопасным, не используйте X forwarding. При его использовании атакующий может аутентифицироваться через ваше подключение SSH для вторжения на X-сервер и, например, отслеживать использование клавиатуры.

1.1.9 Переполнение буфера и Ошибки Функции Форматирования Строк

Как уже обсуждалось в ***1.1.5 Переполнение буфера и Ошибки Функции Форматирования Строк,*** переполнение буфера и ошибки функции форматирвоания строки должны рассматриваться как с точки зрения локальной, так и с точки зрения сетевой безопасности. Как и в случае локальных вариантов этих ошибок, переполнение буфера в сетевых программах, при успешной эксплуатации, используется главным образом для получения прав пользователя root. Даже если в каком-то конкретном случае это не так, атакующий может использовать эту ошибку для получения доступа к непривилегированной учетной записи для эксплуатирования любой другой уязвимости, которяа может уществовать в системе.

Переполнение буфера и ошибки функции форматирования строки, эксплуатируемые через сеть, являются самым частно используемым видом удаленным атак в целом. Эксплойты для них — программы для использования свеженайденных дыр в безопасности — часто публикуются в списках рассылки по безопасности. Для их использования нет необходимости знать детали кода. За эти годы, как показывает опыт, доступность кода эксплойтов способствует увеличению безопасности операционных систем, очевидно, в следствие того, что создатели операционных систем вынуждены закрывать уязвимости в своем программном обеспечении. Благодаря свободному программному обеспечению, каждый имеет доступ к исходному коду (SUSE Linux Enterprise Server поставляется с со всему дсотупными исходными кодами) и каждый, кто найдет уязвимость и эксплойт для нее, может предложить патч для устранения соответствующей ошибки.

1.1.10 Отказ в обслуживании

Цель атаки «отказ в обслуживании» (DoS) — блокирование серверной программы или всего сервера целиком, что может быть достигнуто различными пособами: перегрузка сервера, создание интенсивной нагрузки с помощью «мусорных» пакетов или удаленная эксплуатация переполнения буфера. Часто, единственная цель DoS-атаки — прекращение обслуживания. Однако, как только обслуживание становится недоступным, подключение может стать уязвимым для **атак «человек-по-середине»** (sniffing, TCP hijacking, spoofing) и «отравления» DNS (DNS poisoning).

1.1.11 Человек-по-середине: Sniffing, TCP Hijacjing, Spoofing

Вообще, любую удаленную атаку, когда атакующий вклинивается между обменивающимися информацией хостами, называют **атакой «человек-по-середине»** (man in the middle). Практически все типы атак «человек-по-середине» объединяет то, что жертва обычно не подозревает, что происходит. Существует ножество похожих вариантов, например, атакующий может инициировать запрос на подключение и перенаправить его на целевую машину. Жертва невольно установит соединение с неправильным хостом, потому что машина на другом конце позиционирует себя в качестве легитимного адресата.

Простейшую форму атаки «человек-по-середине» называют **sniffer** — атакующий просто прослушивает проходящий сетевой трафик. В качестве более сложной атаки, атакующий может попытаться захватить уже существующее соединение (hijacking). Чтобы это сделать, атакующему необходимо в течение некоторого времени анализировать пакеты, чтобы быть в состоянии вычислить номера следования TCP, относящиеся к соединению. Когда атакующий захватит роль целевого хоста, жертва обратит внимание на это, поскольку получит сообщение, говорящее, что соединение было прервано из-за ошибки. В действительности, эти протоколы не могут обезопасить от перехвата TCP-соединений посредством шифрования, которое обеспечивает просто процесс аутентификации после установки соединения, облегчая задачу для атакующего.

Spoofing — это атака, при которой пакеты содержат измененные, поддельные исходные данные, обычно IP-адрес. Большая часть активных форм атак полагается на отправку таких поддельных пакетов — что, на машине с Linux, может быть сделано толлько пользователем root.

Многие из упомянутых атак выполняются в сочетании с DoS. Если атакующий видит возможность свалить определенный хост быстро, даже на короткий промежуток времени, это облегчит ему выполнение активной атаки, поскольку хост в течение некоторого времени не сможет помешать ему в этом.

1.1.12 Отравление DNS

Отравление DNS означает, что атакующий повреждает кэш сервера DNS, отвечая ему подмененными ответными пакетами сервера имен, пытаясь передать жертве, желающей получить данные от сервера, определенные данные. Многие серверы поддерживаются доверительные отношения с другими хостами на основании IP-адреса или имени хоста. Атакующему необходимо хорошо понимать фактическую структуру доверительных отношений между компьютерами, чтобы представить себя им в качестве доверенного хоста. Обычно, атакующий анализирует некоторые пакеты, отправленные сервером. Для получения необходимой информации. Атакующему часто должен также сделать целью для своевременных DoS-атак сервер имен. Защитите себя путем использования шифрованных соединений, что позволяет проверить подлинность хоста, к которому идет подключение.

1.1.13 Черви

Червей часто путают с вирусами, но между ними есть одно простое отличие. В отличие от вирусов, червям нет необходимости заражать программу на компьютере для продолжения своего существования. Вместо эого, они созданы специально для наиболее быстрого распространения в сетевых структурах. Черви, созданные в прошлом, Ramen, Lion или Adore, использовали известные уязвимости в серверных программах, таких, как bind8 или lprNG. Защититься от червей относительно просто. Учитывая, что между обнаружением уязвимости и моментом, когда червь атакует ваш сервер, проходит некоторое время, есть достаточно хорошие шансы вовремя обновить программу с уязвимостью. Это принесет пользу только в том случае, если администратор действительно устанавливает обновления безопасности на рассматриваемые системы.

1.2 Некоторые Основные Советы и Уловки по Безопасности

Для того, чтобы управлять безопасностью в достаточной мере, необходимо быть в курсе новых разработок и быть в курсе псоледних проблем безопасности. Одним из лучших способов защитить системы от проблем всех видов является своевременное установка обновленных пакетов, рекомендуемые уведомленями по безопасности. Уведомления по безопасности SUSE публикуются в списке рассылки opensuse-security-announce@opensuse.org. Это основной источник информации об обновлениях пакетов, в который входят члены команды безопасности SUSE. Вы можете подписаться на этот список на странице http://en.opensuse.org/Communicate/Mailinglists.

Предупреждения по безопасности SUSE также доступны через RSS: http://www.novell.com/linux/security/suse_security.xml.

Список рассылки opensuse-security@opensuse.org — хорошее место для обсуждения любых проблем безопасности, представляющих интерес. Подписаться на него можно на той же самой странице.

bugtraq@securityfocus.com — один из самых лучших списков рассылки по безопасности в мире. Очень рекомендуется прочтение этого списка, на отором публикуется примерно 15-20 сообщений в день. Более подробная информация может быть найдена на http://www.securityfocus.com.

Далее представлен список правил, которые могут быть полезны при работе с основными концептиями безопасности:

- Следуя правилам использования наиболее ограниченного набора прав для повседневной работы, избегайте выполнения обычных заданий с правами пользователя root. Это снизит риск получения «кукушкина яйца» и убережет от собственных ошибок.
- Если возможно, всегда используйте шифрованные соединения для работы на удаленной машине. Использование `ssh` (secure shell) вместо `telnet`, `ftp`, `rsh` и `rlogin` должно быть стандартной практикой.
- Избегайте использование методов аутентификации, основанных только на IP-адресе.
- Старайтесь сохранять наиболее важные пакеты, относящиеся к сети, обновленными и подпишитесь на соответствующие списки рассылки для получения уведомлений о новых версиях таких программ (bind, postfix, ssh и др.) То же самое применяется к программному обеспечению, относящемуся к локальной безопасности.
- Измените `/etc/permissions` для оптимизации разрешений на файлы, критичные для безопасности системы. Если вы уберете suid-бит с программы, может случиться так, что она не сможет выполнять свои работу соответствующим образом. С другой стороны, предполагается, что программа также перестанет быть потенциально рискованной в плане безопасности. Можно проделать подобное со всеми каталогами и файлами, запись в которые разрешена всем.
- Отключите абсолютно все службы, которые не требуются серверу для работы должным образом. Это сделает ашу систему более безопасной. Открытые порты, состоянии сокеты которых LISTEN, могут быть найдены с помощью программы `netstat`. Что касается опций, рекомендуется использовать `netstat -ap` или `netstat -anp`. Опция `-p` позволяет увидеть, какой порт занимает процесс с таким именем.

Сравните результаты вывода `netstat` с результатами программы сканирования портов, сделанного снаружи. Превосходная программа для этих целей — `nmap`, которая не только проверяет порты на вашей машине, но иделает выводы относительно служб, которые работают на этих портах. Однако, сканирование портов может быть интерпретировано как акт агрессии, так что не делайте этого без явного одобрения администратора. И наконец, помните, что ажно просмотреть не только порты TCP, но и порты UDP (опции `-sS` и `-sU`).

- Для контроля целостности файлов на вашей системе для надежности, используйте программу AIDE (Advanced Intrusion Detection Environment), доступную в SUSE Linux Enterprise Server. Шифрование базы данных, созданной AIDE, препятствует тому, что кто-то вмешается в работу программы. Кроме того, необходимо сохранять резервную копию этой базы за пределами машины.
- Будьте внимательны при установке любого стороннего программного обеспечения. Были случаи, когда злоумышленник встраивал троянского коня в архив пакета с программным обспечением, но к счастью это быстро обнаружили. Если вы устанавливаете бинарный пакет, убедитесь, что нет никаких неопределенностей с сайтом, с которого он был получен.

  RPM-пакеты в SUSE подписаны с помощью GPG. Вот ключ, использующийся SUSE для подписи:

  ```
  ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>
  Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA
  ```

  Команда rpm --checksig package.rpm показывает, корректны ли контрольная сумма и сигнатура неустановленного пакета. Ищите ключ на первом компакт-диске дистрибутива или на большинстве серверов ключей в мире.
- Регуоярно проверяйте резервные копии системных файлов файлов пользователей. Предположите, что если вы не проверите резерные копии на работоспособность, они в действительности могут быть повреждены.
- Проверяйте файлы логов. При возможности, напишите небольшой скрипт для поиска подозрительных записей. По общему признанию, это отнюдь не тривиальная задача. Поскольку только вы знаете, какие записи подозрительны, а какие таковыми не являются.
- Используйте `tcp_wrapper` для ограничения доступа к конкретным службам, запущенным на машине, что позволит явно контролировать IP-адреса, с которых будет возможен доступ к этим службам. Для получения дополнительной иформации о `tcp_wrapper` обратитесь к man-страницам tcpd и hosts_access (man 8 tcpd, man hosts_access).
- Используйте SuSEFirewall для еще большего увеличения безопасности, обеспеченной `tcpd` (`tcp_wrapper`).
- При создании мер безопасности предусмотрите их избыточность: сообщение, увиденное дважды, гораздо лучше, чем полное отсутствие сообщений.
- Если вы используете suspend-to-disk, предусмотрите шифрование полученного образа с помощью скрипта `configure-suspend-encryption.sh`. Программа создает ключ, копирует его в `/etc/suspend.key` и изменяет `/etc/suspend.conf`, чтобы использовать шифрование для образа.

1.3 Использования Единого Адреса для Отчетов по Безопасности

Если вы обнаружите связанную с безопасностью проблему (пожалуйста, проверьте сначала доступные обновления безопасности), напишите на security@suse.de. Так же необходимо включить подробное описание проблемы и версию затронутого пакета. Вам постараются ответить как можно скорее. Поощряется шифрования письма с помощью pgp. Ключ pgp SUSE:

```
ID:3D25D3D9 1999-03-06 SUSE Security Team <security@suse.de>
```

```
Key fingerprint = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5
```

Этот ключ также доступен для загрузки с http://www.novell.com/linux/security/securitysupport.html.