**Обеспечение безопасности среды Novell NetWare 5**

Много лет NetWare фирмы Novell пользовалась репутацией одной из самых надежных операционных систем из имеющихся на рынке. Пока другие выпускали сетевые ОС, для обеспечения, безопасности которых администратор должен обладать талантом настоящего волшебника, Novell всегда придерживалась той точки зрения, что сетевая операционная система надежной и безопасной должна быть изначально, а права доступа к системным ресурсам нужно предоставлять только по мере необходимости. Но является ли NetWare той самой "нирваной", о которой мы все мечтаем? В Novell хотят, чтобы мы так думали, однако для обеспечения безопасности среды NetWare приходится проделывать гораздо больше работы, чем многие могут себе представить.

В этой статье мы рассмотрим, как можно обезопасить среду NetWare. Обратите внимание на то, что мы остановимся только на ОС NetWare 5.х - прочие продукты фирмы Novell, такие, как BorderManager и GroupWise, имеют свои особенности и тоже нуждаются в принятии тех или иных мер по обеспечению безопасности перед их использованием.

**Безопасность файлов и объектов NDS**

Несмотря на то, что каждая конкретная реализация NDS обладает своими особенностями, администратор должен разбираться в правилах безопасности, применимых ко всем объектам NDS. Уяснив наши рекомендации и освоив несколько практических методов, он должен уметь обеспечить безопасность NDS, по крайней мере, в отношении объектов. Ниже приведены некоторые рекомендации по обеспечению такой безопасности объектов дерева NDS.

По умолчанию объекту Admin предоставлен полный доступ ко всем объектам дерева NDS, поэтому он всегда будет "лакомым куском" для атакующих. Чрезвычайно важно предпринять особые меры предосторожности по отношению к нему. В разных случаях предпринимаемые меры могут различаться, тем не менее существует несколько общих приемов:

Переименуйте объект Admin в соответствии со стандартным соглашением об именовании и поместите его в обычный пользовательский контейнер.

Предоставьте администраторам полномочия, достаточные для выполнения их задач, - и не более.

Используйте переименованную учетную запись администратора только в тех случаях, когда это абсолютно необходимо.

Создайте новый объект с именем Admin, заблокируйте его и ведите аудит данного объекта, регулярно проверяя журнал безопасности.

Все вышесказанное может показаться вам очевидным, но вы удивитесь, узнав, как редко эти рекомендации применяются на практике.

Убедитесь в том, что учетная запись guest удалена - она всегда является объектом для атаки. Обратите внимание на полномочия, наследуемые объектами. Если не используются фильтры наследуемых полномочий (Inheritance Rights Filters - IRF), последние передаются сверху вниз по дереву NDS и права доступа, предоставленные на одном уровне, могут действовать и там, где это не было предусмотрено. В особо запутанных случаях администратор всегда может просмотреть полномочия конкретного объекта, а затем блокировать нежелательные права посредством IRF или установкой явных ограничений. По умолчанию доступ к регистрационному справочнику с правом чтения разрешен всем пользователям, даже тем, кто не зарегистрирован в системе.

Используя предоставленные объекту Public по умолчанию права на просмотр дерева NDS и утилиту CX, атакующий вполне сумеет просканировать атрибуты структуры дерева, что в дальнейшем может быть использовано для получения более полного доступа к системе. Однако возможности этой утилиты существенно ограничиваются запретом объекту Public доступа к объекту Root. Вы должны быть осторожны, изменяя таким образом права доступа, так как некоторым приложениям может потребоваться доступ к объекту Root.

**Безопасность на физическом уровне**

Важный аспект обеспечения безопасности - размещение всех компонентов сети в безопасных местах. Никогда не выставляйте на всеобщее обозрение ваш центр управления сетью (Network Operating Center - NOC). Злоумышленники охотятся за любой информацией, и, когда ее становится достаточно для атаки, не сомневайтесь, рано или поздно она будет предпринята. Убедитесь в наличии резервных источников питания и средств кондиционирования воздуха, поскольку их выход из строя повлечет за собой отказ всей корпоративной сети.

**Защита управляющей консоли**

Если консоль сервера не используется, ее нужно заблокировать. В утилите Scrsaver.nlm, поставляемой в составе ОС NetWare 5.0, реализован новый метод блокировки серверной консоли: в отличие от предыдущих версий утилиты Console Lock утилита Scrsaver.nlm для обеспечения безопасности обращается к службе NDS. Для того чтобы разблокировать консоль, вы должны ввести имя пользователя и пароль NDS. Затем Scrsaver по списку контроля доступа (Access Control List - ACL) проверяет, обладает ли данный пользователь правами доступа к конкретному серверу и, если это так, разблокирует консоль. Дополнительная информация об этом содержится в документе TID (Technical Information Document) № 2941164, доступном на Web-сайте Novell.

**Удаленное администрирование**

Несмотря на то что любой администратор сети может привести целый ряд причин, по которым удаленное администрирование сервера необходимо, к его практической реализации следует подойти со всей серьезностью. В состав ОС NetWare 5.x входит традиционное приложение Rconsole и написанная на языке Java утилита удаленного администрирования RconsoleJ. Обе программы имеют один и тот же недостаток - работают поверх незашифрованных соединений.

Требования безопасности, предъявляемые к такого рода приложениям, очень высоки, поскольку, если злоумышленник получит доступ к управляющей консоли, он сможет сделать почти все, что ему нужно. Существует большой набор средств для создания привилегированных учетных записей и соответствующей модификации существующих. Тем не менее консольный доступ необходим почти всегда.

И Rconsole и RconsoleJ являются источниками дополнительного риска по следующим двум причинам:

Модули удаленного администрирования, загружаемые при запуске системы, используют пароли, сохраняемые в обычном текстовом файле. Хотя компания Novell и предлагает средства для их шифрования, администраторы часто продолжают хранить списки паролей в виде простых текстовых файлов, являющихся прекрасной целью для возможной атаки. Пароли необходимо шифровать всегда. Хоть это и не обеспечивает стопроцентной безопасности, но все же лучше, чем ничего.

Соединения, устанавливаемые Rconsole и RconsoleJ, небезопасны, так как большая часть информации при этом открыто передается в текстовом виде. Перехватывая пакеты, взломщик может получить важную информацию, недоступную иным способом.

Если удаленное администрирование вам абсолютно необходимо, возможны два пути ее защиты:

Изучите и используйте программное обеспечение для удаленного администрирования, передающее информацию поверх защищенных соединений.

Используйте встроенные приложения NetWare при соблюдении следующих условий:

Чтобы избежать перехвата пакетов, вместо концентраторов применяйте правильно сконфигурированные коммутаторы.

Храните в строжайшем секрете пароль удаленного администрирования и регулярно изменяйте его.

Убедитесь в том, что после использования консоль остается заблокированной.

Никогда не применяйте незашифрованные пароли.

Не запускайте сеанс удаленного администрирования с помощью исполняемого файла, расположенного в разделе DOS. В этом случае простая перезагрузка позволит злоумышленнику получить пароль.

**Secure Console**

Для того чтобы в какой-то степени нейтрализовать атаку, если взломщик получит доступ к консоли, используйте утилиту Secure Console. Она повышает уровень безопасности, предотвращая загрузку любых модулей, кроме расположенных в каталогах SYS:\SYSTEM или C:\NWSERVER. Кроме того, она предотвращает доступ с клавиатуры в системный отладчик и запрещает производить изменение системных даты и времени.

**Контекст Bindery**

Уже много лет существуют приложения, позволяющие перехватывать информацию Bindery. Эти средства способны обманывать NetWare и перехватывать пересылаемые по сети пакеты. Такое средство может установить фальшивое соединение с сервером, заставив его "думать", что запросы исходят от рабочей станции администратора. С помощью этих приложений атакующий вполне в состоянии изменить стандартные права доступа пользователя на права доступа администратора и получить в свое распоряжение все сетевые пароли.

Часто приложения или службы, в особенности унаследованные, требуют включения поддержки контекста Bindery, не оставляя других альтернатив администратору. Если нельзя заменить эти приложения или службы на совместимые с NDS, атаку можно предотвратить, предприняв ряд мер, описанных ниже в разделе "Безопасность NCP". Если включение поддержки Bindery не является необходимым, все контексты должны быть удалены.

**Механизм репликации**

Одно из преимуществ использования NDS заключается в возможности разбиения корневой БД на отдельные разделы и обеспечения избыточности путем создания их дубликатов. Наибольшей степени избыточности, по Novell, можно достичь, как минимум, тремя репликами каждого раздела NDS, но при этом вы не обязаны использовать компьютеры с ОС NetWare для хранения копий базы данных. С помощью продукта e-Directory фирмы Novell вы можете располагать ваши реплики на других платформах.

**Версии Directory Services**

Служба Directory Services представлена модулем ds.nlm и несколькими дополнительными модулями. Из-за значительных различий ее версий строгое соблюдение общепринятых стандартов становится насущной необходимостью. Так как служба справочника - самый важный компонент ОС NetWare, многие администраторы не решаются осуществлять обновление этих модулей, что может вылиться в другие проблемы, включая и те, которые возникают при попытке объединить различные версии NetWare в одно дерево. Тем не менее нужно отметить, что тестирование новых модулей перед их использованием следует проводить обязательно, так как известны случаи, когда в службах справочника обнаруживались серьезные ошибки.

**Безопасность NCP**

Фирменный протокол Novell - NetWare Core Protocol (NCP) - применяется в сетях NetWare для организации взаимодействия с клиентскими машинами. В ряде случаев NCP-пакеты могут быть подменены злоумышленником, что позволяет ему получить доступ к информации о различных компонентах сети. Некоторые средства для осуществления этого процесса стали достоянием общественности. Самое известное и мощное среди них - Pandora. Эта утилита предназначена исключительно для получения информации с серверов NetWare.

Противостоять такого рода вторжениям можно, отклоняя NCP-пакеты неверной длины и с неправильными компонентами, а также устанавливая на клиентах и серверах значение уровня подписи NCP-пакетов, равное 3.

**Аудит**

Одним из наиболее важных аспектов политики безопасности является аудит. Средство Novell AuditCon позволяет отслеживать все события в среде NetWare, начиная с ее файловой системы и кончая NDS. Поэтому его следует регулярно использовать. Необходимо вести аудит аутентификации супервизора, изменений объектов NDS, сценариев регистрации в системе и полномочий пользователей.

В дополнение к стандартным средствам Novell некоторые сторонние фирмы тоже выпустили утилиты для аудита среды NetWare; эти продукты включают в себя средства как обнаружения вторжения, так и наблюдения за соответствием пользовательских полномочий принятой политике безопасности.

**Полномочия пользователей**

Методика назначения пользовательских полномочий должна быть тщательно продумана еще на стадии планирования сети NetWare. Ниже приводится список компонентов, которым при выработке этой методики необходимо уделить особое внимание. Помните о необходимости компромисса: слишком строгая политика безопасности приведет к увеличению доли ошибочных отказов в доступе, а слишком мягкая - к образованию "дыр" в системе защиты. Итак:

Одно из распространенных средств отражения атак - ограничение числа активных сеансов для каждой отдельной учетной записи. Запрет многократной регистрации с одинаковыми учетными атрибутами поможет предотвратить атаку в рабочие часы, по крайней мере на время сеанса того или иного пользователя. Нужно принять во внимание, что некоторые версии службы справочника не вполне адекватно реагируют на прекращение пользовательского сеанса связи, в результате чего часто возникает путаница с освобождающимися соединениями. Но в последних версиях службы справочника эта ошибка исправлена, поэтому и в NetWare 5.x и в Directory Services 8 все работает нормально.

Ограничив время доступа к определенным учетным записям, вы снизите вероятность атак на эти записи в определенные часы. Обычно эта мера применяется в рабочее время.

Процесс обнаружения вторжений включает в себя аспекты, которые следует принять во внимание. Это максимальное число неудачных попыток регистрации и время сброса блокировки учетной записи. Первый параметр определяет, сколько попыток дается пользователю для регистрации в системе до тех пор, пока его учетная запись не будет заблокирована. Заблокированная после последней неудачной попытки учетная запись может быть, затем разблокирована автоматически или администратором. Этот параметр по возможности должен иметь минимальное значение. Время сброса блокировки учетной записи обозначает промежуток времени, в течение которого учетная запись пользователя будет заблокированной до тех пор, пока не произойдет автоматического сброса блокировки. В большинстве случаев этому параметру следует присваивать максимальное значение, вследствие чего станет невозможно зарегистрироваться без вмешательства администратора.

Пользовательские шаблоны помогают администраторам создавать учетные записи, базируясь на корпоративной политике безопасности. При отсутствии шаблонов, как правило, возрастает вероятность ошибки, особенно в условиях нехватки времени. Используйте пользовательские шаблоны в соответствии с организационной схемой NDS.

Администратор может устанавливать ограничения на аутентификацию для определенных узлов. Данный метод, в частности, предотвращает попытки аутентификации с рабочих станций, не принадлежащих локальной сети. Это, правда, потребует лишних усилий от администратора, но впоследствии обеспечивает очень высокий уровень безопасности. Метод наиболее эффективен тогда, когда рабочие станции пользователей являются стационарными; в случае же с мобильными станциями при реализации данного метода администратору предстоит решить многие проблемы.

Ограничение сроков действия учетных записей особенно эффективно при использовании временных учетных записей. Даже если отсутствует постоянное администрирование, такие записи через определенный промежуток времени становятся недоступными.

Часто используется и считается весьма эффективным способом атаки на сеть угадывание пароля. Короткие пароли для такого типа атак более уязвимы. Обычно устанавливают минимальную длину пароля в 5-6 символов. Можно рассмотреть и другие случаи применения паролей.

Параметром принудительной смены пароля задается значение, определяющее, через сколько дней пользователю придется сменить пароль. По истечении указанного времени ему будет предоставлено определенное количество попыток регистрации для смены пароля до того, как доступ к учетной записи будет заблокирован. Разблокирование учетной записи потребует вмешательства администратора. Обычно рекомендуется присваивать этому параметру значение, равное 60-90 дням.

С помощью параметра предоставляемых попыток доступа (grace-logins) можно определить, сколько раз подряд пользователю разрешается пытаться зарегистрироваться для смены пароля. Если присвоить слишком большое значение этому параметру, система безопасности подвергается риску, являющемуся оборотной стороной метода принудительной смены пароля. Поэтому присваивайте этому параметру минимальное значение.

**Web-серверы и FTP-серверы Novell**

Во время инсталляции Web-служб Novell в раздел тома SYS записывается некое количество сценариев и средств управления приложениями, в частности NetBasic, Perl и Sewse, которые могут представлять опасность в том случае, если злоумышленник попытается использовать их в своих целях. Необходимо обязательно удалить их оттуда, чтобы в будущем они не стали источником возникновения проблем.

Обычно не рекомендуется использовать FTP-серверы в корпоративной среде. Но если это неизбежно, размещайте FTP-службу и данные на собственном отдельном томе. Не держите их на томе SYS.

**Замечание об уровне безопасности C2**

Требования к программно-аппаратным средствам в отношении обеспечиваемого ими уровня безопасности A, B, C и D описаны в документе Trusted Computer System Evaluation Criteria (TCSEC), опубликованном Национальным центром компьютерной безопасности (NCSC) США. Данный документ обычно именуют Оранжевой книгой. Это одна из нескольких книг известной "цветной" серии руководящих документов Агентства национальной безопасности США (National Security Agency - NSA). В соответствии с положениями Оранжевой книги основой обеспечения безопасности на уровне C2 является метод дискреционного управления доступом (Discretionary Access Control - DAC). Система не сертифицируется в качестве отвечающей требованиям уровня C2 до тех пор, пока не получит "добро" от NSA. Такие системы должны обеспечивать достаточно высокую степень безопасности.

Фирма Novell не только отказалась от идеи претендовать на официальное подтверждение соответствия ОС NetWare 5.х требованиям безопасности уровня С2, но даже не удосужилась подготовить документ, описывающий, каким образом можно привести ее продукт в соответствие с этими требованиями. Означает ли это, что в компании считают такой уровень безопасности излишним? Или, может быть, руководство фирмы не уверено в том, что ее продукт сможет успешно пройти сертификационные испытания? Однозначного ответа у нас нет.

**Удостоверяющие центры Novell**

В ОС NetWare 5.0 не только появилась поддержка технологии асимметричного шифрования для обеспечения безопасности сеансов связи клиентов с серверами - теперь администраторы NetWare могут использовать свои собственные удостоверяющие центры (Certificate Authority - CA), интегрированные со службой NDS. Продукт Novell Certificate Server 2.0 поддерживает спецификацию электронной почты S/MIME (Secure MIME) для клиентов Microsoft Outlook 98/2000, Novell GroupWise 5.5 (c пакетом расширения) и Netscape Messenger. Этим же продуктом поддерживаются Web-браузеры Microsoft Internet Explorer 4.x и 5.x, а также Netscape Navigator 4.x.