**Как дать отпор хакерам**

Первое, что приходит в голову многим системным администраторам, когда они думают о защите своих сетей от атак злоумышленников из Интернета, это слово "брандмауэр". Брандмауэры (сетевые экраны) - неотъемлемая часть инфраструктуры защиты сети, однако просто установить брандмауэр и надеяться на лучшее - опасно и глупо. Если не выбрать надлежащую конфигурацию серверов и не придерживаться сильной стратегии защиты, то шансы на успех у атакующих вашу сеть значительно повышаются. Как уже неоднократно писалось, большинство злоумышленников нападает с внутренней стороны брандмауэра. Это недовольные сотрудники фирмы или хакеры, нашедшие лазейку в системе. По этой причине к защите каждой сети нужно подходить очень внимательно и не ограничиваться предотвращением доступа из Интернета.

Еще одно опасное заблуждение заключается в том, что серверы будто бы уже поставляются с необходимыми средствами обеспечения безопасности. Между тем, в защите каждой сетевой операционной системы имеются многочисленные пробелы, и чтобы считать свой сайт действительно защищенным, их необходимо ликвидировать. Отсутствие строгой стратегии обеспечения безопасности интрасети и серверов Интернета может усугубить ситуацию. Чтобы получить бессонницу, администратору сети достаточно попытаться установить последние поправки к системе защиты сетевой ОС.

Сделать жизнь сотрудников, отвечающих за работу сети, более спокойной помогут инструментальные средства сканирования сетевой и системной защиты в сочетании с хорошо спланированной стратегией безопасности и ПО обнаружения нарушителей. Эти продукты сканируют сетевые серверы по заданному расписанию и автоматически выводят отчеты, позволяя быстро обнаружить ошибки в конфигурации, неправильно инсталлированное (с точки зрения защиты) серверное ПО и пробелы в защите (преднамеренные или нет), и принять необходимые меры.

В лаборатории ZD Internet Lab были испытаны три инструментальных средства защиты на базе Windows NT. К сожалению, компания Network Associates не смогла вовремя представить последнюю версию своего сканера CyberCop Scanner (прежнее название Ballista), Axent Technologies отказалась принять участие в обзоре, сославшись на предстоящее обновление своего продукта, а фирма Netect не подготовила NT-версию продукта Netective (ко времени написания обзора она проходила бета-тестирования, но версия для ОС Solaris уже существует).

**Итоговый анализ**

Продукт ISS Internet Scanner 5.2 мы выбрали по многим причинам. Он оказался наиболее полным в плане поиска проблем в системе защиты и предлагал наиболее исчерпывающие решения каждой проблемы. Это ПО выявило все недостатки в защите, обнаруженные остальными двумя продуктами, и дополнило их десятками других найденных пробелов. Функциональные возможности вывода отчетов в Internet Scanner 5.2 оказались просто феноменальными, а сами отчеты детальны и легко читаемы. Они предназначены не только для технических специалистов. В сводных отчетах для руководителя вопросы защиты сети поясняются и становятся намного понятнее. Сканирование сети в Internet Scanner 5.2 производится быстро и полно, а результаты мы смогли использовать для генерации множества отчетов и, при необходимости, обращаться к оригинальным данным.

**Слабые места систем**

Существуют следующие, наиболее распространенные, слабые места, характерные для многих сетевых операционных систем:

1) Слабая защита по паролю.

2) Доступ через анонимный FTP.

3) Неиндексированные каталоги WWW.

4) Разрешенная функция Finger.

5) Разрешенные банеры Telnet/sendmail.

6) Разрешенная учетная запись Guest.

7) Неправильная конфигурация RPC.

8) Ошибки в IIS .bat и .cmd.

9) Уязвимость TFTP.

10) Неверная конфигурация NFS.

ПО Internet Scanner 5.2 компании Internet Security Systems (Атланта) - самый давний из протестированных нами продуктов оценки защиты, и большой опыт положительно сказывается на его работе. На нас произвели впечатление простота установки данной программы, превосходные средства вывода отчетов и широкая поддержка платформ. Internet Scanner - компонент защиты семейства продуктов SAFEsuite компании Internet Security Systems. Кроме этого, SAFEsuite включает в себя компоненты выявления вторжения RealSecure и инструмент для детального анализа конфигураций серверов Unix System Security Scanner (S3). Разрабатывается версия S3 для Windows NT. Internet Scanner функционирует в сетях Windows NT 4.0, AIX, HP-UX, Solaris и Linux. Продукт может выявлять "дыры" в защите, недостатки в конфигурации Windows NT Server и Workstation, машин Windows 95 и серверов Unix. Все проверки системы и сканирование выполняются через TCP/IP в локальной сети.

Установить ПО Internet Scanner оказалось нетрудно. Мы загрузили самую последнюю его версию с веб-узла ISS и легко выполнили процесс инсталляции. После установки ПО на нашем сервере Windows NT нам потребовалось только скопировать файл ключа ISS в каталог Internet Scanner, после чего можно было начинать сканирование. Сервер ключа ISS передал нам лицензионный ключ по электронной почте. Этот ключ определяет, какие именно компоненты Internet Scanner будут доступны пользователю. Таким образом, добавление функциональных возможностей (таких, как сканирование брандмауэра) представляет собой простую и быструю онлайновую процедуру.

Пользовательский интерфейс Internet Scanner понравился нам больше всех. "Мастер" создания сеанса значительно упрощает настройку и запуск процедуры сканирования. Основное окно с вкладками спроектировано настолько ясно, что мы смогли сразу легко загрузить несколько сеансов, ускорив тем самым процесс сканирования. Выполнение поверхностного теста сканирования нашего сервера Windows NT Server заняло у Internet Scanner всего 21 секунду, после чего мы получили страницу с результатами - детальным списком обнаруженных проблем и предлагаемых решений. В этом тесте Internet Scanner выявил на нашем сервере 113 ошибок конфигурации и пробелов защиты. Из них было выделено пять проблем высокой степени риска, 10 - средней и 98 - низкой.

Не устраняя ни одной из обнаруженных проблем, мы продолжили процесс, выполнив сканирование среднего уровня того же сервера Windows NT Server. На этот раз сканирование заняло немногим более трех минут, и было найдено 114 уязвимых мест. Пять проблем продукт отнес к высокому риску, 11 - к среднему и 98 - к низкому.

Наконец, глубокое сканирование нашего сервера Windows NT заняло более 5 минут и показало наличие в нашей конфигурации 115 ошибок. На этот раз число проблем высокого риска увеличилось до шести, проблем со средним риском по-прежнему насчитывалось 11, а проблем низкого риска - 98. Затем мы занялись своим сервером RedHat Linux 5.1, также начав с поверхностного сканирования. Как и в случае аналогичного теста Windows NT, этот процесс занял 20 секунд. Как ни странно, он обнаружил только одну проблему в защите: у нас была включена функция Finger. Эта проблема была отнесена к категории низкого риска.

Сканирование среднего уровня сервера RedHat 5.1 потребовало около четырех минут и обнаружило девять пробелов в защите: одну средней степени риска (разрешенный доступ через анонимный FTP) и восемь проблем низкой степени риска. Во время теста с углубленным сканированием продукт нашел 15 проблем, на что ушло примерно 7 минут. Две проблемы были отнесены к средней степени риска, а остальные 13 - к низкой.

Средства вывода отчетов в Internet Scanner произвели на нас очень сильное впечатление. Генерируемые в формате Crystal Reports или HTML, разнообразные готовые формы отчетов Internet Scanner должны удовлетворить требования любого сетевого администратора. Если же потребуется создать свои собственные формы, то в Internet Scanner для них легко построить шаблоны. В технических отчетах об уязвимости системы защиты перечислены проблемы, указаны машины, на которые они влияют, предлагаются решения и даже даются ссылки на места в Интернете, где можно найти соответствующие поправки и корректировки. В отчетах для руководителей суммируются характеристики защиты всей сети.

Internet Scanner 5.2 соединяет в себе превосходный пользовательский интерфейс, сильные средства создания сеансов и большое число стандартных отчетов. Двухуровневая схема лицензирования (795 $ за лицензию на сканирование 10 серверов и 4995 $ за лицензию на сканирование всей подсети класса C) делает пакет Internet Security Systems доступным как для малых, так и для крупных компаний.

Инструмент оценки защиты NetGuard компании Network Guardians позиционируется как приложение, полностью основанное на Java. Между тем, когда мы инсталлировали его на своем сервере Windows NT, то обнаружили, что программный код для сканирования Windows NT Workstation и Server на самом деле является "родным" кодом Windows и может работать только в Windows NT. В файле README поясняется, что инструменты сканирования на Java для платформы Windows NT будут доступны в ближайшее время. Конечно, Java - превосходный инструмент для приложений, которые должны работать на разных платформах, но мы не уверены, что это актуально для данной категории продуктов. Нам кажется, что администраторов гораздо больше интересуют реализованные в них средства сканирования и возможность выполнения с любой сетевой рабочей станции.

NetGuard оказался единственным из рассматриваемых продуктов, способным обнаруживать уязвимые места в защите Macintosh. Как и Internet Scanner, NetGuard использует для сканирования (локального и удаленного) хост-систем протокол TCP/IP. Между тем, NetGuard не выявил такого количества пробелов в защите, как Internet Scanner, хотя основные "дыры" от него не ускользнули.

Мы загрузили NetGuard с веб-узла Network Guardians Website, получив код аутентификации, который позволяет войти в защищенную область узла с загружаемым программным обеспечением. Такой подход позволяет компании регулярно обновлять свой продукт. Кроме того, мы загрузили оттуда последнюю версию (1.16) Java Runtime Edition (JRE) для Windows NT. После инсталляции обоих компонентов можно было приступать к сканированию. Пользовательский интерфейс NetGuard произвел на нас приятное впечатление. Он хорошо продуман и работает как любое другое Windows-приложение, хотя и реализован на основе Java. Все его элементы, включая командные кнопки, таблицы и вкладки, функционировали правильно.

NetGuard завершил поверхностное сканирование нашего сервера Windows NT менее чем за 30 секунд, выявив три пробела в защите. Все они были отнесены к проблемам низкой степени риска. Сканирование среднего уровня заняло 3,5 минуты, а число обнаруженных проблем увеличилось до пяти. Четыре из них были отнесены к низкой степени риска, а одна - к высокой. При выполнении детального сканирования сервера Windows NT (выполнявшегося более четырех минут) NetGuard сообщил о тех же пяти проблемах.

Поверхностное сканирование сервера RedHat 5.1 потребовало 30 секунд и дало информацию о четырех слабых местах в системе защиты. Три проблемы были отнесены к низкому риску, а одна - к высокому. Сканирование среднего уровня (4 минуты) сервера RedHat 5.1 выявило уже шесть проблем: одну - высокой степени риска, одну - средней, и четыре - низкой. Углубленное сканирование сервера RedHat 5.1 заняло целых 9 минут (самое большое время во всех наших испытаниях). На этот раз обнаружилось 11 проблем в защите: две - высокой степени риска, три - средней и шесть - низкой.

Средства вывода отчетов в NetGuard нам понравились. В правой части экрана выводится наглядный список проблем со ссылками на рекомендации по их устранению. К этому же отчету можно обратиться и в формате HTML. NetGuard - самый дешевый из протестированных нами продуктов. За 199 $ вы получаете возможность сканировать 16 хост-систем, а за 2499$ предоставляется лицензия на неограниченное сканирование. Поскольку инструмент работает практически на любой аппаратной платформе, это превосходный выбор для компаний, применяющих разные аппаратные конфигурации.

Нам понравился GUI-интерфейс NetGuard на базе Java, но предлагаемые данным продуктом средства сканирования следовало бы усилить. Между тем, если вам нужны защищенные серверы Macintosh, то NetGuard остается единственно доступным вариантом.

**Kane Security Analyst 4.04**

Продукт Kane Security Analyst компании Security Dynamics Technologies входит в семейство инструментов защиты SecurSight. Kane Security Analyst может оценивать защиту автономного сервера Windows NT или, если приобрести расширенную лицензию, всего домена Windows NT. В отличие от двух других протестированных нами продуктов, Kane Security Analyst предназначен только для сканирования серверов Windows NT и Novell NetWare. Сканирования серверов Unix или машин Windows 95/98 он не выполняет.

Мы загрузили пакет Kane Security Analyst на своем сервере Windows NT с инсталляционного диска CD-ROM, после чего можно было приступать к работе. При первом запуске программы она выполнила поиск доменов и серверов нашей сети Windows NT. Затем на экране появилось главное окно. Пользовательский интерфейс Kane Security Analyst спроектирован удачно. Каждая из четырех кнопок в нижней части экрана выполняет один из четырех шагов по оценке защиты системы: устанавливает стандарт защиты, проверяет ее, анализирует степень риска и выводит отчет. Кроме того, предусмотрены кнопки быстрого вызова большинства функций Kane Security Analyst, таких, как оценка на соответствие стандарту защиты C2 (C2 Security Evaluation), вывод на экран карты отчета и т.д.

ПО Kane Security Analyst не предусматривает поверхностного, среднего и углубленного сканирования, как Internet Scanner и NetGuard. Программа поставляется с одним заданным по умолчанию шаблоном сканирования, именуемым Best Default Practices. Этот шаблон сравнивает защиту вашего сервера с практикуемыми в отрасли методами защиты. Естественно, можно создать и собственный шаблон, отвечающий специальным требованиям.

Скорость сканирования произвела на нас благоприятное впечатление. Анализ всей системы, включая тест раскрытия пароля, потребовал менее 30 секунд, после чего нам была представлена "карта отчета" со списком выполненных тестов и оценкой для нашего сервера. За ограничение учетных записей наш сервер Windows NT получил 85%, за длину пароля - 56%, за контроль доступа - 86%, за мониторинг системы - 42%, а за целостность и конфиденциальность данных - 50%. В целом наша система получила среднюю оценку, равную 63%, и попала в "критический" диапазон.

После завершения сканирования можно получить набор детальных отчетов (в формате Crystal Reports). Выбрав отчет (или все отчеты), его нетрудно сгенерировать, распечатать или сохранить в файле (в разных форматах), однако мы были разочарованы тем, что Kane Security Analyst не предлагает средств вывода отчетов непосредственно в формате HTML.

Kane Security Analyst оказался самым дорогим из рассматриваемых нами продуктов: 695 $ за сервер. Поскольку он может сканировать серверы только той платформы, на которой выполняется, это достаточно высокая цена. Конечно, вряд ли это остановит компанию, которую волнует уязвимость защиты, однако не следует забывать о том, что данный продукт не сканирует хост-системы Unix.

В целом Kane Security Analyst можно считать превосходным инструментальным средством для сканирования серверов Windows, но в неоднородной сетевой среде он не может конкурировать с Internet Scanner 5.2.

**Как отгоняют хакеров в Microsoft**

Директор корпорации Microsoft по защите информации Говард Шмидт (Howard Schmidt) вполне удовлетворен функциональными характеристиками ПО Internet Scanner компании Internet Security Systems (ISS). После четырехмесячного периода оценки Microsoft выбрала Internet Scanner по трем причинам: из-за надежности продукта, его постоянного обновления и сильного персонала поддержки. "Internet Scanner смог выявить больше уязвимых мест, чем некоторые другие оцениваемые нами продукты, - отметил Шмидт. - У этого продукта сильная поддержка, и он постоянно обновляется в соответствии с вновь обнаруживаемыми "дырами" в защите, а сотрудники компании всегда готовы ответить на вопросы и выявляют потенциальные проблемы раньше, чем наши собственные специалисты".

Технический персонал ISS продолжает работать в тесном контакте с сотрудниками Microsoft. Они общими усилиями воздвигают заслон для хакеров. На Шмидта произвели сильное впечатление и средства вывода отчетов, предлагаемые Internet Scanner: "Конечно, есть хорошие инструменты, способные идентифицировать уязвимые места в системе, но возможность собрать информацию воедино и представить в осмысленной форме - одно из превосходных качеств именно этого продукта".

Internet Scanner был установлен на всех системах Microsoft в конца мая, хотя его тестирование завершилось еще в 1997 году. Теперь Microsoft нуждается в полном комплекте защиты и рассматривает Internet Scanner как один из основных его элементов. "Для нас большую ценность представляют продукты, способные взаимодействовать с ISS. Например, крайне желательна система обнаружения нарушителей, которая могла бы выводить отчеты для этого продукта, с тем, чтобы можно было получать осмысленные выводы".

Internet Scanner предлагает превосходные отчеты по результатам сканирования. Они легко читаются и сразу дают четкую картину состояния защиты сервера. У Kane Security Analyst необычный интерфейс администрирования и структура отчетов, но он выявил не все пробелы в защите нашего сервера Windows NT.