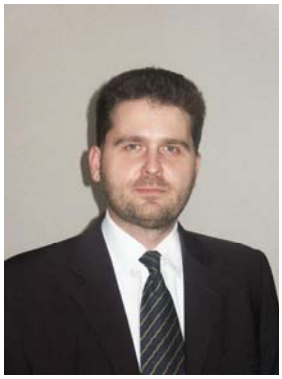
ДИАГНОСТИКА ЗАЩИЩЕННОСТИ КОРПОРАТИВНЫХ ТОЧЕК ДОСТУПА[1]

Алексей Пастоев, CISSP
apastoev@kerberus.ru



Сегодня уже не надо разъяснять значение защиты компьютерных систем. Данная тема тем более актуальна, что число компьютерных преступлений все возрастает, а предприятиям по-прежнему недостает уверенности в надежности предпринятых мер защиты. Для оценки эффективности таких мер нужно периодически проводить аудит ИТ-инфраструктуры. Однако, каким бы он качественным ни был, сомнения все равно остаются. Что же делать? Как удостовериться в действенности предпринятых мер защиты?

Основная задача практической диагностики состоит в оценке возможности для представителей групп риска — неэтичных конкурентов, нелояльных сотрудников и хакеров — получить несанкционированный доступ к корпоративным компьютерным ресурсам. Иными словами, практическая диагностика ориентирована на проверку средств защиты конфиденциальности информации и должна включать проверку всех путей удаленного доступа к корпоративным системам, которые могут быть использованы злоумышленником. Как правило, речь идет о точках доступа к Internet, о точках доступа к компьютерным системам из локальной сети, о точках доступа по коммутируемым каналам (модемные соединения), о беспроводных локальных сетях Wi-Fi, о Web-сайтах в сетях intranet/Internet. Последние выделены в отдельный пункт потому, что для проверки их надежности требуются специальные методики. Применение только одних сканеров для Web-серверов не позволяет достичь качественных результатов: сканер не найдет такие уязвимости, как «зашитый» пароль в Java-приложении, использование скрытых полей в формах и недостаточный контроль вводимых данных, а также «забытые» комментарии программистов.

Практическая диагностика защищенности компьютерных систем позволяет: идентифицировать скрытые уязвимости компьютерных систем; проверить правильность настроек безопасности; проверить эффективность систем обнаружения атак; определить, к каким данным потенциальный злоумышленник может получить доступ; повысить внимание руководства компании к вопросам компьютерной безопасности.

ВОПРОСЫ ПРАКТИЧЕСКОЙ ДИАГНОСТИКИ

[1] Статья опубликована в журнале «Открытые Системы» №10, октябрь 2004. Во время написания статьи автор работал в компании «Ernst and Young»

Практическая диагностика дает ответы на вопросы:

- какие дополнительные усилия и ресурсы необходимы для обеспечения адекватного уровня защищенности;
- имеются ли несанкционированные устройства или сервисы в компьютерных сетях;
- насколько эффективны процедуры внесения изменений в компьютерные системы, включая установку «заплат»;
- насколько эффективны процедуры управления доступом в системы;
- соблюдаются ли корпоративные политики компьютерной безопасности;
- насколько сотрудники компании осведомлены о правилах безопасного использования компьютерных систем.

МЕРЫ ПРЕДОСТОРОЖНОСТИ

В нашу рабочую группу практической диагностики систем защиты обычно не включаются специалисты, имеющие хакерское прошлое, однако они должны владеть, как минимум, всеми известными техниками, которыми потенциально могут воспользоваться злоумышленники. Их цель — выявить все уязвимости, существующие на момент проверки. Практическая диагностика защиты корпоративных точек доступа Internet заключается в целеустремленных попытках проникновения в корпоративную ИТ-инфраструктуру из Internet путем имитации действий представителей из групп риска: хакеров, неэтичных конкурентов, нелояльных сотрудников. Обычно она занимает 2-5 дней в зависимости от количества систем, подключенных к Internet, и заканчивается подготовкой детализированного отчета.

При проведении диагностики защиты корпоративных точек доступа Internet неизбежно возникают дополнительные риски. Для предотвращения возможных нежелательных последствий соблюдается ряд правил.

- Организуется тесное взаимодействие с заказчиком диагностики на всех этапах — начиная от определения объема работ и до подготовки финального отчета.
- В рабочую группу включается представитель заказчика.
- Ежедневно предоставляется письменный отчет о проделанной работе и достигнутых результатах, согласовывается дальнейшая программа действий.
- Заказчик немедленно оповещается об обнаружении серьезных уязвимостей.
- С заказчиком дополнительно согласовываются действия, способные повлиять на нормальную работу систем, а также время их проведения.
- Используются процедуры контроля полноты и качества выполняемых тестов.
- Результаты диагностики, включая рабочие материалы и отчеты, хранятся в безопасном месте.
- Договор об оказании услуг обязательно содержит раздел о конфиденциальности.

ПРЕДВАРИТЕЛЬНЫЙ СБОР ДАННЫХ

Практическая диагностика защиты корпоративных точек доступа Internet начинается с определения, какие первоначальные знания об объекте тестирования будут использоваться. Диагностику можно делать «вслепую», т.е. при наличии ограниченной информации об объектах исследования или при ее полном отсутствии. Преимущество данного подхода заключается в том, что он моделирует реальную ситуацию, а также позволяет оценить эффективность внутренних процедур по выявлению атак и реагированию на них. А основным недостатком является потребность в дополнительной координации действий (для соблюдения требований конфиденциальности). Тем не менее, диагностика, которую не ожидает получить ИТ-служба, часто обеспечивает более убедительные основания для пересмотра и укрепления мер компьютерной защиты в организации и привлечения внимания руководства.

Далее необходимо пополнить свои знания об объекте проверки из общедоступных источников. Какими бы незначительными ни были первоначальные сведения об объекте диагностики (например, визитная карточка сотрудника, содержащая, как правило, название организации, номера телефонов, адрес электронной почты и название Web-сайта компании), ее бывает достаточно для начала сбора дополнительной информации. Для этого используются общедоступные поисковые сервисы Internet, например Google или «Яндекс». На этом этапе можно составить список сотрудников компании, их адресов электронной почты, номеров ICQ и много другой полезной информации. Адреса электронной почты могут, например, подсказать правила образования имен учетных записей пользователей. Часто в электронных форумах можно найти сообщения, оставленные сотрудниками компании, которые дают ценные сведения об объектах тестирования. Как-то в открытом доступе мы обнаружили описание схемы корпоративной точки доступа Internet, оставленное нерадивым сетевым администратором. Дополнительные сведения, например, адреса корпоративного прокси-сервера и несанкционированных сетевых сервисов, можно узнать с помощью поисковых сервисов Internet, задавая в качестве параметра поиска IP-адреса.

Ряд поисковых сервисов Internet предоставляет возможность просматривать интересующие документы, сохраненные в памяти поисковой машины. Это позволяет собрать дополнительную информацию до момента обращения к объекту тестирования напрямую, совершенно незаметно для систем защиты.

Далее можно приступать к работе с сервисами WHOIS и DNS для получения максимального объема информации об объекте тестирования. Обычно мы выполняем комплексный поиск всех данных по хостам путем передачи зон на DNS-серверах компании, включая не только IP-адреса, названия доменов, но и любую информацию о доменных именах, которая может содержать привлекательные для взломщиков сведения, такие, как тип системы (например, HINFO). В случае невозможности пакетной передачи зон (zone transfer) используются специальные средства, например утилита domainsearch.pl позволяющая определять имена хостов на индивидуальной основе по словарю. Такие

имена, как ftp, checkpoint, winnt, proxy и router позволяют сделать предположение о типе используемой операционной системы, установленном программном обеспечении и функциональном назначении системы. Далее следует разобраться, как организована точка доступа Internet, и составить ее схему.

На основе списка доменов и IP-адресов путем трассировки пакетов к каждому IP-адресу выявляются маршруты доступа в сеть. В дополнение к стандартным средствам применяются специализированные трассировки к открытым TCP или UDP портам в случае, если стандартная трассировка заблокирована. Это позволяет выявить как «официальные» маршруты доступа, так и те, о которых компания-заказчик может не знать. По результатам этого этапа составляется развернутая схема маршрутов доступа, которая потребуется для анализа потенциальных путей проникновения в корпоративную сеть из Internet.

СКАНИРОВАНИЕ ТОЧКИ ДОСТУПА К СЕТИ

Выявление доступных сетевых сервисов имеет ключевое значение для определения используемых операционных систем и прикладных программ. Часть доступных сетевых служб можно определить по названию хоста и собранной ранее дополнительной информации. Точный результат по всем доступным сервисам дают различные типы сканирования портов TCP и UDP:

- **Стандартное сканирование** пакетами TCP и UDP.
- **Скрытое сканирование** пакетами FIN, SYN и ACK. Присвоение этих меток пакетам TCP зачастую позволяет пакетам, посылаемым взломщиками, оставаться незамеченными. Кроме этого, некоторые простейшие средства контроля доступа не способны препятствовать прохождению таких пакетов во внутренние системы.
- **Фрагментированное сканирование**. Представляет собой модификацию других методов и позволяет пользователю разбивать пакет на несколько более мелких фрагментов IP. Многие средства контроля доступа не способны адекватно реагировать на подобные действия и выявлять фрагментированные пакеты при их прохождении через контрольное устройство.
- **Сканирование обратной идентификации TCP**. Системы, использующие протокол идентификации (RFC 1413), допускают раскрытие имени пользователя для инициатора любого процесса, подключаемого через TCP, даже если указанный процесс не активирует подключение, имеется возможность определять инициаторов процессов по каждому из прослушиваемых сервисов.
- **Атака с использованием возврата сообщений через FTP**. Протокол FTP (RFC 959) позволяет поддерживать «прокси»-подключения, и если напрямую подключенная к Internet система может работать с протоколом FTP, обеспечивая возврат пакетов, то существует возможность сканирования портов других систем через ftp-сервер. В зависимости от схемы сети, этот метод может использоваться для сканирования портов, доступ к которым блокирует сетевой экран.

Эффективным средством сканирования портов, без сомнения, является утилита nmap, распространяемая компанией Insecure.Com. Процесс сканирования может занимать достаточно длительное время. Поэтому, учитывая огра-

ничения на срок проведения диагностики, мы выполняем сначала предварительное сканирование по ограниченному набору портов, а затем — полное, чтобы не упустить из виду ни одного доступного сервиса.

После определения доступных сетевых сервисов собираются уточняющие сведения о них путем подключения к открытым портам и взаимодействия с этими сервисами.

ОПРЕДЕЛЕНИЕ ТИПА ОПЕРАЦИОННЫХ СИСТЕМ И СЕТЕВЫХ СЕРВИСОВ

Для подготовки целенаправленных действий с целью преодоления систем защиты необходима точная идентификация удаленных систем. Используя составленный список доступных портов в каждой из подключенных к Internet систем, мы пытаемся получить из тестируемого объекта как можно больше информации путем сбора заголовков сетевых сервисов и запросов к ним. Информация, предоставляемая такими службами, как SNMP, finger, rusers, SMTP, LDAP или NetBIOS, позволяет определить детальную конфигурацию и информацию о пользователях для каждой системы. Эта сведения крайне важны и могут оказать самое непосредственное содействие в обходе средств защиты тестируемых систем.

В дополнение к перечисленным методам при необходимости можно применить так называемую «TCP-дактилоскопию» — исключительно эффективную технологию, позволяющую быстро и с высокой степенью точности определять тип операционной системы. Для «TCP-дактилоскопии» обычно достаточно доступа к одному прослушиваемому сервисному порту. Соответственно, имеется возможность точно определять операционную систему тестируемого ресурса путем отправки специально созданных пакетов на один открытый порт (например, 53).

Полученные данные систематизируются (см. таблицу) и используются на следующих этапах и при подготовке отчета.

ТАБЛИЦА. ПРИМЕР СИСТЕМАТИЗАЦИИ ДАННЫХ

IP-адрес	Порт	ОС	Заголовок сетевого сервиса
XXX.XXX.XXX.1	23/telnet 22/SSH	Solaris 7	SUN Solaris 7 Login: SSH-1.99-OpenSSH_3.4p1
XXX.XXX.XXX.2	25/SMTP	Novell Netware	GroupWise Internet Agent 6.0.3 (C)1993, 2003 Novell, Inc.
XXX.XXX.XXX.3	80/HTTP	FreeBSD	Apache/1.3.28 (Unix) PHP/4.3.3
XXX.XXX.XXX.4	25/SMTP 85/HTTP 110/POP3 445/SMB	Windows 2000 Server	ESMTP Service (Lotus Domino) Microsoft-IIS/5.0 +OK Microsoft Exchange POP3 server version 5.5.2448.8 ready
XXX.XXX.XXX.5	21/FTP 80/HTTP	Axis Camera	220 Axis 2100 Network Camera 2.32 Jun 11 2002 ready. Server: Boa/0.92o

Многие корпоративные точки доступа к Internet находятся под наблюдением систем обнаружения вторжений (intervention detection system, IDS), достаточно эффективных против малоквалифицированных хакеров и позволяющих быстро заблокировать источник подозрительных действий, однако не спасаю-

щих от действий квалифицированного злоумышленника. Более того, в руках профессионального хакера IDS может стать средством проведения атаки типа «отказ в обслуживании» (Denial of Service, DoS).

В зависимости от режима работы IDS (блокировка источника подозрительных действий или просто фиксация факта атаки) и требуемой степени скрытности работ, мы применяем технику модифицирования атак, задача которой — не попасть под «шаблон», который IDS использует для выявления подобных действий. Для этого используются цепочки прокси- или SOCKS-серверов для скрытия источника атаки, фрагментирование пакетов, подмена адресов в IP-пакетах.

По моему опыту, системы IDS не предотвращают проникновений, а лишь увеличивают время, необходимое на подготовку успешной атаки. В случае, если атака производится через шифрованные соединения (например, по протоколам SSL или SSH), то сетевые системы IDS вообще не в состоянии ни зафиксировать факт атаки, ни блокировать ее источник.

ОПРЕДЕЛЕНИЕ УЯЗВИМЫХ МЕСТ

Анализ систематизированных данных на предмет наличия уязвимых версий сетевых сервисов позволяет выявить потенциально слабые места. Для определения уязвимых мест мы также используем собственные коммерческие средства. Кроме этого, для многих задач требуется дополнительная ручная работа — собственные разработки предназначены в основном для выявления уязвимых мест, о которых разработчики программного обеспечения часто забывают или просто не учитывают. Примером подобных средств могут служить программы обхода механизмов сетевой аутентификации, переполнения буфера и «столкновения» программ для получения привилегированного доступа к Unix-системам, усовершенствованные методы взлома паролей и специальные программы для получения доступа к удаленной системе.

Применение программ-сканнеров уязвимостей, даже лучших коммерческих версий, не позволяет выявить многие серьезные пробелы в защите систем. Многие из них не обеспечивают однозначных результатов из-за наличия ложных положительных и отрицательных результатов и возможности двойного толкования отчетов. Необходимо тщательно анализировать результаты применения каждой такой программы и, по мере возможности, вручную проверять наличие трудно выявляемых узких мест для подтверждения достоверности результатов.

Ввиду относительно статичного характера коммерческих сканирующих программ эти продукты часто не способны выявлять недавно обнаруженные уязвимости, поэтому необходимо отслеживать появление сведений о новых средствах атак на малоизвестные и относительно новые уязвимые места, особенно в части проблем, выявленных уже после выпуска последних версий автоматических сканирующих программ.

Пока еще ни одна программа автоматического сканирования уязвимостей не способна выявлять возможность комплексных атак, использующих сразу несколько обнаруженных в разных системах уязвимых мест с низкой или

средней степенью риска для получения привилегированного доступа. Это означает, что сканер может выявить несколько уязвимых мест с низкой или средней степенью риска, но не способен определить степень вероятности того, что комбинированная атака на эти уязвимые места приведет к прорыву систем защиты.

Одной из самых «лакомых» уязвимостей является наличие несанкционированных сетевых сервисов. На практике часто встречается ситуация, когда сотрудники компании устанавливали на компьютерах, к которым имелся доступ из Internet, свои собственные Web-сайты, камеры, ICQ, сетевые компьютерные игры и другое программное или аппаратное обеспечение без санкции подразделения информационной безопасности. Такие сервисы, как правило, имеют широкий спектр уязвимостей, причем некоторые несанкционированные сервисы бывает довольно сложно обнаружить, например, виртуальный сайт наподобие www.<имя домена>.com, расположенный на одном сервере с корпоративным сайтом.

Критическим компонентом любого межсетевого фильтра является способность предотвратить атаки типа «отказ в обслуживании» защищаемых им компьютерных систем. Для оценки эффективности мер защиты от атак такого рода мы не создаем реальную ситуацию с отказом в обслуживании, а лишь получаем подтверждение возможности создания подобной ситуации. Конечная цель заключается в оценке степени надежности сетевой среды без нарушения штатной работы компьютерных систем.

Уязвимости типа «исчерпание пропускной способности канала доступа» (Distributed denial of service, DDoS) не могут быть исследованы в рамках практической диагностики защищенности корпоративных точек доступа Internet из-за своей специфики — они затрагивают ИТ-инфраструктуру провайдера и не могут выполняться без его согласия.

ПОЛУЧЕНИЕ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Получив необходимую информацию об объекте исследования можно перейти к кульминационной стадии диагностики, задача которой — проникновение в системы в демилитаризованной зоне (DMZ) и в расположенную за ней корпоративную сеть.

В первую очередь здесь следует попытаться использовать уязвимости, которые основаны на ошибках в настройках систем или логических ошибках в программах и не влияют на нормальную работу системы, в отличие от уязвимостей типа «переполнение буфера». При этом следует учитывать страну, где находится объект проверки. Необходимо, например, иметь хорошие словари паролей, специфичных для родного языка администраторов и пользователей систем.

Далее следует выделить время на тестирование уязвимостей, возникающих из-за «человеческого фактора». Например, использование слабых паролей, использование одного пароля для разных систем, «забытые» и тестовые учетные записи. Автоматизированные средства проверки качества паролей, например, «Hydra», позволяют вести ускоренный параллельный поиск

слабых паролей в большом количестве сетевых служб, включая telnet, ftp, pop3, imap, smb, smbnt, http, https, http-proxy и др.

Проверка содержимого публично доступных ресурсов системы, например, ftp-сервера, позволяет обнаружить файлы, которыми обмениваются сотрудники территориально удаленных подразделений и администраторы систем, имена пользователей, пароли, технические инструкции по подключению к корпоративным сервисам.