



Заключение по результатам теста на проникновение
в информационную систему
ОАО «Север Золото»

**Заключение по результатам теста на проникновение
в информационную систему
ОАО «Север Золото»**

Введение

Тест на проникновение в информационную систему из глобальной сети Интернет является эффективным способом, который позволяет оценить защищённость информационной системы и обнаружить не только отдельные уязвимости, но и проверить надёжность существующих механизмов защиты в целом. Тест на проникновение максимально приближен к реальности и позволяет аудиторам смоделировать большую часть угроз информационной безопасности, воздействующих на информационную систему. В данном заключении приводятся результаты теста на проникновение в информационную систему ОАО «Север Золото».

Техническое задание

Согласно Техническому заданию по проведению теста на проникновение в информационную систему ОАО «Север Золото» (далее – Заказчика), компании Acolyte были предоставлены следующие данные об информационной системе:

1. Перечень IP-адресов хостов, образующих внешний периметр информационной системы Заказчика (подсеть 168.192.200.0/28).
2. Перечень адресов корпоративной электронной почты в домене severzoloto.ru, представляющий собой репрезентативную выборку по сотрудникам из различных структурных подразделений.

Согласно Техническому заданию по проведению теста на проникновение в информационную систему Заказчика, применялась следующая методика, позволяющая наиболее полно смоделировать действия потенциального нарушителя:

1. Пассивный сбор сведений об информационной системе Заказчика из открытых источников.
2. Активный сбор сведений об информационной системе Заказчика (подключение к хостам внешнего периметра).
3. Проверка возможности проникновения в информационную систему Заказчика при помощи использования уязвимостей сетевых служб, запущенных на хостах внешнего периметра.
4. Проверка возможности проникновения в информационную систему Заказчика при помощи реверсивной троянской программы.

Согласно Техническому заданию, о ходе выполнения работ по тесту на проникновение в информационную систему Заказчика регулярно сообщалось представителям отдела информационной безопасности Заказчика. Сотрудникам отдела информационных технологий, ответственным за администрирование информационной системы, не было сообщено о факте выполнения таких работ.

Описание злоумышленника

В качестве потенциального нарушителя информационной безопасности ОАО «Север Золото» рассматривается лицо или группа лиц, состоящих или не состоящих в сговоре, которые в результате умышленных или неумышленных действий могут реализовать разнообразные угрозы информационной безопасности, направленные на информационные ресурсы и нанести моральный и/или материальный ущерб интересам ОАО «Север Золото».

В качестве угроз информационной безопасности рассматриваются базовые угрозы нарушения конфиденциальности и целостности информации, а также угроза отказа в обслуживании инфраструктуры информационной системы. Сводная характеристика вероятного нарушителя приведена в таблице.

Классификация	Характеристика
По мотиву нарушения информационной системы	Нарушение угрозы целостности, конфиденциальности, доступности в корыстных или иных целях
По уровню информированности и квалификации нарушителя	<p>Обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем</p> <p>Обладает достаточными знаниями для сбора информации, применения известных эксплоитов и написания собственного программного обеспечения для осуществления атаки</p> <p>Не является авторизованным пользователем информационной систем</p>
По месту действия	<p>Без непосредственного (физического) доступа на территорию объекта (внешний нарушитель).</p> <p>Нарушитель действует удаленно, через сеть Интернет</p>

Анализ защищенности информационных ресурсов

Перед началом работ по проведению теста на проникновения был составлен примерный «профиль информационной системы» – приблизительное описание корпоративных сервисов, предоставляемых информационной системой сотрудникам ОАО «Север Золото» и пользователям глобальной сети Интернет. Такая предварительная оценка позволяет сразу же выделить основные направления, подлежащие анализу в первую очередь. Было сделано предположение, что типовые корпоративные сервисы данной информационной системы – это система электронной почты, корпоративный сайт или портал, система доступа удаленных клиентов, а также служебные подсистемы – например, службы DNS, NTP и – ключевой компонент – подсистема средств защиты.

Пассивный сбор сведений

Пассивный сбор сведений об информационной системе проводился при помощи общедоступных сетевых сервисов – службы DNS, службы WHOIS, а также программ traceroute, tracerpath и т.п., web-интерфейс к которым предоставляют многие сайты (таким образом, IP-адрес потенциального нарушителя остаётся неизвестным для атакуемой системы). Утилита host позволяет получить перечень всех доменных имён исследуемой зоны severzoloto.ru:

```
sms% host -l -t any severzoloto.ru
severzoloto.ru name server ns1.severzoloto.ru.
severzoloto.ru name server ns2.severzoloto.ru.
severzoloto.ru has address 168.192.200.11
severzoloto.ru mail is handled by 10 mail.severzoloto.ru.
severzoloto.ru mail is handled by 20 mold.severzoloto.ru.
severzoloto.ru has SOA record ns1.severzoloto.ru. root.severzoloto.ru.
2005073101 1800 900 2592000 900
mail.severzoloto.ru is an alias for ns2.severzoloto.ru.
www.severzoloto.ru is an alias for ns1.severzoloto.ru.
telcom-gw.severzoloto.ru has address 168.192.200.1
gate.severzoloto.ru has address 168.192.200.10
ns1.severzoloto.ru has address 168.192.200.11
ns2.severzoloto.ru has address 168.192.200.12
realsecure.severzoloto.ru has address 168.192.200.13
mold.severzoloto.ru has address 168.192.200.14
```

Анализ доменных имён хостов, находящихся в зоне severzoloto.ru, позволяет сделать предположение о функциональном назначении хостов, имеющих записи в базе DNS. Таким образом, не проводя активного сканирования всех портов для каждого из исследуемых хостов, существует возможность получить сведения об информационной системе. Предположительно, хост 168.192.200.1 – это шлюз провайдера телекоммуникационных услуг, хост 168.192.200.10 является корпоративным шлюзом ОАО «Север Золото», 168.192.200.11 – сервером DNS и

WWW, 168.192.200.12 – вторичным сервером DNS, на 168.192.200.13 установлен сенсор системы обнаружения вторжений ISS RealSecure, 168.192.200.14 – резервный почтовый сервер, 168.192.200.15 – широковещательный адрес. Информация, полученная при помощи программ traceroute и tracert, позволяет составить примерную карту сети и сделать предположения об установленных межсетевых экранах и правилах фильтрации сетевого трафика.

Предположительно, не обнаруженный в базе DNS хост 168.192.200.4 является маршрутизатором, который контролирует демилитаризованную зону. Путём отправки «случайных» пакетов с адресов сервера acolyte.ru из заданного диапазона была предпринята попытка пассивного определения удалённой ОС при помощи программы r0f.

Активный сбор сведений

Во время активного сбора информации было проведено сканирование хостов всего диапазона при помощи программы nmap. Для снижения риска обнаружения «нарушителей» средствами предположительно установленной в исследуемой подсети ISS RealSecure сканирование проводилось в течение длительного времени, с большими интервалами между сканированием отдельных портов.

Были определены версии программного обеспечения сетевых служб на исследованных хостах. Проведённое сканирование показало корректность исходных предположений о профиле информационной системы. После этого была выполнена проверка достоверности полученной информации. С большой долей уверенности можно было утверждать, что сокрытие или изменение версий программного обеспечения сетевых служб администраторами информационной системы не проводилось.

Анализ уязвимостей сетевых служб

Поиск уязвимостей в программном обеспечении сетевых служб не дал положительных результатов, были предприняты лишь контрольные запуски эксплоитов на службы SMTP и WWW для проверки чувствительности сенсора ISS и возможного блокирования IP-адреса, с которого производился запуск эксплоита, средствами маршрутизатора или межсетевого экрана. Подсистема защиты никак не отреагировала на активные попытки атаки, адрес «нарушителя» заблокирован не был.

Запуск реверсивной троянской программы

Следующим этапом выполнения теста на проникновение являлась рассылка троянской программы пользователям информационной системы согласно согласованному перечню адресов электронной почты. Необходимо отметить, что при помощи популярных поисковых систем (www.yandex.ru, www.google.com)

потенциальный нарушитель может получить адреса электронной почты сотрудников ОАО «Север Золото», которые по тем или иным причинам оказались опубликованы в сети Интернет, и использовать эту информацию для более эффективной атаки при помощи троянской программы. Была разработана троянская программа, позволяющая в случае её запуска на компьютере пользователя получить удалённый (через Интернет) доступ к ресурсам данного компьютера и корпоративной сети с правами пользователя, запустившего программу. Троянская программа является реверсивной – то есть, самостоятельно иницилирующей запросы к своему управляющему серверу (установленному на сервере acolyte.ru), который сообщает ей последовательность команд для выполнения на компьютере пользователя, а в ответ получает результат выполнения этих команд. Это позволяет использовать троянскую программу в сетях с трансляцией сетевых адресов (NAT). Троянская программа обходит распространённые средства защиты в типовой конфигурации, используемые в корпоративных сетях – персональные межсетевые экраны, системы обнаружения вторжений, прокси-серверы с авторизацией доступа и т.п. Троянская программа в полной мере использует особенности архитектуры ОС Windows, установленной на рабочей станции пользователя, что позволяет существенно уменьшить объем исполняемого модуля и обеспечить высокий уровень функциональных возможностей программы.

Троянская программа была разослана пользователям в виде сжатого в ZIP-архив и прикрепленного к письму исполняемого файла. Письмо было якобы отправлено одним сотрудником ОАО «Север Золото» другому и содержало предложение запустить трёхмерную версию компьютерной игры «Тетрис». Замаскированную таким образом троянскую программу в течение двух рабочих дней после рассылки запустили 8 из 20 пользователей, чьи адреса электронной почты находились в перечне, предоставленном компании Acolyte. Одна из рабочих станций (адрес 10.100.3.64, маска подсети 255.255.254.0), которая, судя по времени работы (uptime), не выключалась по окончании рабочего дня, была выбрана в качестве исходной точки для организации атаки. Далее троянская программа загрузила со своего управляющего сервера код эксплоита для службы RPC (для ОС Windows 2000 и Windows XP) и провела атаку на контроллер домена (адрес 10.100.1.10, маска подсети 255.255.254.0), в котором находилась данная рабочая станция, а также другие серверы и рабочие станции, перечень которых был получен с контроллера домена. Контроллер домена оказался уязвим к данной атаке, вследствие был получен полный административный доступ к командной строке контроллера домена. Чтобы зафиксировать факт проникновения, троянская программа получила команду создать в домене пользователя dsadmin с привилегиями администратора домена. Далее при помощи программы pwdump, загруженной троянской программой на рабочую станцию, с которой проводилась атака, была получена база паролей пользователей домена (более 1200 учётных записей). Дальнейший подбор этих паролей показал, что пароли большей части учётных записей как рядовых пользователей, так и администраторов

информационной системы Заказчика являются слабыми и могут быть получены атакой по словарю и перебором за короткое время. Уязвимыми к данной атаке оказались также сервер, на котором была развёрнута СУБД Oracle (адрес 10.100.1.13), сервер доступа RAS (адрес 10.100.1.17), резервный контроллер домена (адрес 10.100.1.11), файловый сервер (адрес 10.100.1.15), а также более 60 рабочих станций. По приблизительным оценкам (на основе информации, полученной с контроллера домена), в информационной системе Заказчика 12 серверов и не менее 400 рабочих станций. Как правило, столь значительное количество уязвимых хостов говорит об отсутствии сервера обновлений Windows Update, который должен быть развернут в информационной системе. Далее была предпринята попытка использовать скомпрометированные пароли администраторов информационной системы для доступа к коммутаторам Cisco, на которых была собрана локальная вычислительная сеть информационной системы Заказчика. Комбинация логина cisco и пароля sugerka (от одной из административных учётных записей) позволила получить доступ уровня 15 (максимально возможный) к консоли управления каждого из 6 коммутаторов сети (с адресами 10.100.1.1, 10.100.3.1, 10.100.5.1, 10.110.1.1, 10.110.3.1, 10.110.5.1).

Выводы

1. Внешний периметр информационной системы Заказчика защищён достаточно надёжно: регулярно выполняется установка обновлений программного обеспечения сетевых служб, конфигурация служб соответствует требованиям информационной безопасности. Тем не менее, сетевые службы предоставляют потенциальному нарушителю достоверную служебную информацию, что может быть использовано при организации атак на внешний периметр.
2. Система обнаружения вторжений установлена в конфигурации по умолчанию, её настройка неэффективна и не обеспечивает адекватный уровень реакции на явно выраженную сетевую активность нарушителя.
3. Общая архитектура информационной системы Заказчика, конкретные технические решения по обеспечению информационной безопасности и низкая квалификация пользователей информационной системы не обеспечивают требуемый уровень защиты, что позволило осуществить успешный запуск троянской программы.
4. Уровень защищённости серверов и рабочих станций информационной системы Заказчика – низкий. Отдельно необходимо отметить низкий уровень защиты критически важных серверов: контроллера домена и сервера СУБД, в которой хранится важная для бизнеса информация.
5. Анализ скомпрометированной базы паролей пользователей показал низкую стойкость паролей как обычных пользователей, так и администраторов системы.

Рекомендации

1. Включить скрытие служебной информации, предоставляемой сетевыми службами пользователям.
2. Выполнить тонкую настройку системы обнаружения вторжений.
3. Развернуть в информационной системе сервер обновлений Windows Update, включить автоматическое обновление на всех серверах и рабочих станциях.
4. Развернуть в информационной системе сетевую систему обнаружения вторжений, которая позволила бы протоколировать подозрительную сетевую активность и оперативно реагировать на подобные инциденты.
5. Разработать парольную политику, включающую в себя требования по стойкости паролей, правила хранения и периодической замены ключевых фраз. Недопустимо использование единого пароля для администрирования всех ресурсов информационной системы. К паролям административных учётных записей должны предъявляться особые требования по стойкости.
6. Разработать и реализовать на практике программу обучения пользователей вопросам информационной безопасности.