Атаки на системы обнаружения беспроводных атак

Сергей Гордейчик
gordey @ ptsecurity.com

Содержание

Введение

Системы обнаружения беспроводных атак (Wireless Intrusion Detection System, WIDS) пока не настолько популярны, как их проводные аналоги, но современные тенденции позволяют предсказывать рост числа их внедрений. Положительным фактором является интеграция подобных программ с активным сетевым оборудованием и осознание руководством рисков, связанных с несанкционированным использованием беспроводных устройств. Последнее приводит к увеличению числа инсталляций WIDS даже в сетях, где беспроводные сети не используются. В связи с этим у специалистов в области безопасности возникает необходимость оценить не только качественные характеристики того или иного продукта, но и прогнозировать возможное негативное влияние от его внедрения на безопасность корпоративной сети.

В данной статье описываются результаты исследований систем обнаружения беспроводных атак с точки зрения специалиста в области безопасности приложений. Обнаруженные ошибки проектирования в статье не обсуждаются, поскольку их устранение требует от производителя существенных трудозатрат.

Архитектура WIDS

Современная система обнаружения беспроводных атак представляет собой достаточно сложное решение, построенное на основе двух- или трехзвенной архитектуры, зачастую использующее Web-технологии.

Основу WIDS составляют сенсоры, выполняющие функцию сбора беспроводного трафика в режиме мониторинга, и, возможно, его обработку. Сенсоры могут быть реализованы на базе ОС линейки Windows или "специализированных программно-аппаратных комплексов" (в большинстве случаев - Linux). Как правило, сенсоры представляют собой достаточно интеллектуальные устройства, поддерживающие TCP/IP и обладающие развитыми интерфейсами управления.

Сенсоры взаимодействуют с компонентом сбора данных (сервером), передают ему информацию об обнаруженных атаках или перехваченных пакетах. Сервер обрабатывает поступившую информацию, выполняет функции обнаружения атак и корреляции событий безопасности. В качестве хранилища информации обычно используется стандартная СУБД. Для управления системой и мониторинга событий используются консоль управления, выполненная в виде "толстого" или "тонкого" клиента.

Таким образом, WIDS представляет собой распределенную систему, потенциально уязвимую для атак, лежащих не только в беспроводной плоскости.

Источники угроз

Чтобы придать статье тень наукообразия, можно сформировать "модель злоумышленника", то есть определить основные антропогенные источники угроз. Для WIDS к таким относятся внешние злоумышленники, взаимодействующие с системой через радиоэфир, внутренние злоумышленники, имеющие доступ к локальной сети, и операторы, обладающие некоторыми ограниченными возможностями по управлению компонентами системы.

Архитектура типичной системы обнаружения беспроводных атак, и рассматриваемые в статье векторы атак приведены на рисунке 1.

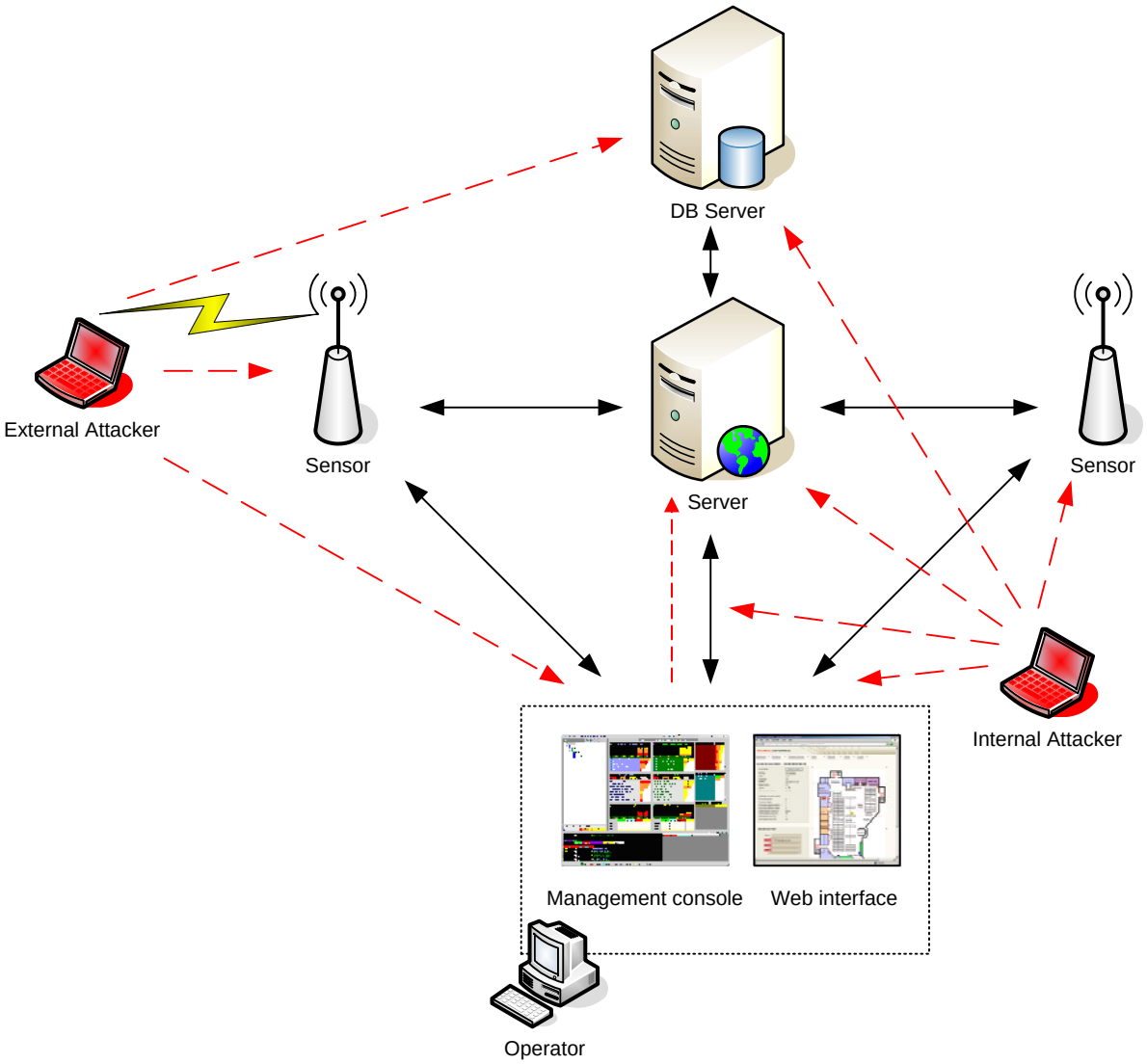

Рисунок 1. Архитектура системы обнаружения беспроводных атак

Взлом через воздушный зазор

Основным механизмов воздействия внешних злоумышленников на систему обнаружения беспроводных атак является создание фреймов 802.11, обработка которых приведет к нестандартным ситуациям. Опыт эксплуатации проводных систем обнаружения атак [1], а также багтрека Ethereal/Wireshark показывает, что наличие уязвимостей в

"вивисекторах" сложных протоколов является вещью вполне обыденной. Конечный автомат канального уровня 802.11 достаточно непрост для того, чтобы вводить в заблуждение разработчиков. Уязвимости в Kismet [2], а также последние публикации [3] об уязвимостях в драйверах беспроводных клиентов заставляют задуматься о вероятном наличии подобных проблем в сенсорах WIDS. Однако это имеет слабое отношение к теме статьи.

Поскольку данные, полученные из недоверенного источника, сохраняются в базе данных, существует вероятность их некорректной обработки, и как следствие - возможность проведения злоумышленником атак типа "внедрение операторов SQL" (SQL Injection). Добавление к строковым полям пакетов, сохраняемых в СУБД, специальных символов позволяет терминировать исходный SQL запрос и добавить к нему операторы, контролируемые злоумышленником. Практически такая атака может быть реализована путем создания ложных точек доступа или одноранговых сетей с SSID вида:

`;insert into ...

Существенное, но преодолимое ограничение на эксплуатацию данного вида уязвимости накладывает длина SSID (32 байта).

В настоящее время подобная уязвимость обрабатывается в рамках политики ответственного разглашения, и возможно, будет опубликована позже. Однако никто не мешает читателю с помощью функции трассировки СУБД проверить реакцию WIDS на команды типа

iwconfig ath0 mode master essid ';--

Ещё одной распространенной Web-уязвимостью, характерной для систем обнаружения беспроводных атак, является Межсайтовое выполнение сценариев (Cross-Site Scripting, XSS). Информация об обнаруженной атаке отображается в консоли управления, в качестве которой зачастую используется Web-браузер. Соответственно, если злоумышленник укажет в качестве SSID магическую последовательность символов:

"><script>alert()</script>

в браузере оператора или администратора отработает сценарий, контролируемый злоумышленником. В этом случае 32 байта предоставляют достаточный резерв для того, чтобы указать в качестве источника сценария внешний сервер. Результаты такой атаки могут быть

самыми разнообразными - от кражи данных для аутентификации до выполнения некоторых действий по настройке WIDS вместо оператора. Подобная уязвимость была устранена в Web-интерфейсе сервера Airmagnet Enterprise [4]. Условия сохраненного XSS возникали при отображении SSID в списках контроля доступа Enterprise Server:

https://<servername>/Amom/Amom.dll/BD

В случае использования "толстого" клиента ситуация может усложняться. Например, консоль управления AirMagnet для отображения информации об атаке использует внедренный объект Internet Explorer и вставляет в HTML-шаблон SSID точки доступа (или клиента), нарушавшей политику безопасности. Если браузер работает в зоне безопасности Local Machine, внедрение сценариев может привести к серьезным последствиям. Так, например в Windows до XP Service Pack 2 открытие локального HTML файла практически аналогично запуску исполняемой программы. Подробнее о рисках, связанных с использованием в приложениях объекта Internet Explorer, работающего в зоне безопасности My Computer можно узнать из [5] и [6]. Во многих WIDS Web-сервер управления использует аутентификацию типа Basic, что повышает вероятность успеха атак типа CSRF. Однако данная уязвимость настолько распространена, что не стоило её даже упоминать.

Естественно, выполнение этих атак требует, чтобы злоумышленник обладал информацией о типе используемой WIDS, но этот вопрос достаточно хорошо освещен в публикации [7].

Атаки в локальной сети

В отличии от внешнего злоумышленника, внутренний пользователь имеет гораздо большие возможности. Поскольку интерфейсы управления сенсорами и серверами WIDS представляют собой полнофункциональные Web-интерфейсы, злоумышленник с высокой степенью вероятности может обнаружить в этих приложениях весь спектр атак из Web Application Consortium Threads Classification [8].

В качестве примеров можно привести уязвимости [9], в Cisco WLSE и так далее. В интерфейсе управления сенсорами AirMagnet SmartEdge Sensor

также была обнаружена уязвимость типа XSS, возникающая при просмотре журналов аудита:

https://<sensorip>/AirMagnetSensor/AMSensor.dll/XH

WebServer Log

Для осуществления атаки в данном случае используется имя пользователя, вводимое при прохождении аутентификации. Отраженный вариант XSS присутствует в сообщениях об ошибках:

http://<sensor IP>/xss<script>alert()</script>

https://<sensor IP>/xss<script>alert()</script>

Еще одним вектором атак, которым может воспользоваться внутренний злоумышленник, является сетевое взаимодействие между компонентами системы, такие как сбор данных с сенсоров, сохранение событий в СУБД, удаленное управление и просмотр событий.

Естественно данный трафик является достаточно критичным для того, чтобы производители позаботились о его защите с помощью таких надежных механизмов как SSL.

Однако забота об удобстве пользователей заставляет производителей использовать самоподписанные сертификаты и не задействовать механизм их проверки. Например, консоль управления Airmagnet без лишних вопросов воспринимает практически любой сертификат. Это позволяет злоумышленнику, реализовавшему условия "человек посередине" расшифровывать трафик (включая пароли пользователей), передаваемый между консолью управления и сервером с помощью общедоступных средств, таких как ettercap или Cain [10]. Ниже приведен пример перехваченного и расшифрованного трафика.

```
[Client-side-data]
GET /AMom/AMom.dll/UA HTTP/1.1
Accept: */*
AMUser: admin <STATIONID>
AMBuild: 4694
User-Agent: AirMagnet
Host: <serverip>
Connection: Keep-Alive
Authorization: Basic YWRtaW46MTExMTEx
```

```
[Server-side-data]
HTTP/1.1 200 OK
Date: Mon, 20 Mar 2006 12:53:12 GMT
Server: Apache/2.0.52 (Win32) mod_ssl/2.0.52 OpenSSL/0.9.7a
Content-Length: 301
Keep-Alive: timeout=15
Connection: Keep-Alive
Content-Type: text/html

[Server-side-data]
<html>
      3     2     AirMagnetSensor  111111     16777215   1          0

      1111111111111111111111111111111111111111111111111111111111111
1111  1     admin111111     16777215   1          0
      1111111111111111111111111111111111111111111111111111111111111
1111  3     AirMagnetSensor2 111111     16777215   1          0
            0                          </html>
```

Кроме этого, WIDS может работать с активным сетевым оборудованием, например коммутаторами, используя небезопасные сетевые протоколы, такие как SNMPv1, что тоже дает определенные преимущества злоумышленнику.

Атаки со стороны оператора

В большинстве WIDS уровня предприятия реализована функция разграничения доступа. Пользователи могут иметь права на выполнение только определенных операций, например – только просмотр событий, или зона их полномочий может быть ограничена определенными группами сенсоров (здание, этаж).

При наличии уязвимостей в интерфейсе управления данная группа пользователей имеет возможность повысить свои привилегии в рамках системы обнаружения атак или всей сети, если уязвимость достаточно серьезна.

В процессе тестирования Highwall Enterprise Server и Highwall EndPoint 4.0.2.11045 были обнаружены множественные уязвимости типа Cross-Site Scripting и SQL Injection. Пользователь, имеющий права на изменение объектов системы (например, имени сенсора WIDS или

рабочей станции, на которой установлен Highwall EndPoint) может внедрить в страницы сервера операторы Javascript и перехватить данные авторизации более привилегированного пользователя, или выполнить от его имени действия по настройке WIDS.

Функция просмотра информации о точках доступа и зданиях содержит уязвимость типа SQL Injection, что позволяет оператору выполнять на сервере СУБД команды языка SQL. Поскольку в качестве сервера выступает Microsoft SQL Server и приложение работает с ним используя высокие привилегии, злоумышленник имеет большие возможности по развитию атаки.

Вместо заключения

В заключении хотелось бы дать некоторые тривиальных рекомендации для специалистов, выбирающих или развертывающих систему обнаружения беспроводных атак.

1. Проверьте реакцию системы на нестандартный трафик в беспроводной сети. Несколько примеров такого трафика было приведено в статье. Дополнительно можно воспользоваться различными фузерами, например [11].

2. Обратите внимание на уровень привилегий, используемый WIDS для работы с СУБД. Если при этом используется учетная запись суперпользователя, последствия атак могут быть весьма серьезными.

3. При проектировании сетевой инфраструктуры для WIDS учитывайте требования к разделению сетей. Выносите управляющий трафик в отдельный сегмент/VLAN.

4. Отключайте неиспользуемые протоколы удаленного управления сенсорами. Использование доисторического telnet в 2006 году нашей эры может быть оправдано только при построении honeypot.

5. Просканируйте сетевые интерфейсы сенсоров и серверов WIDS с помощью сканера уязвимостей, поддерживающего Web-приложения. Для организации Web-сервера вполне может использоваться старая версия Apache (или другого приложения), содержащего уязвимости. Гарантирую, что в большинстве случаев вы будете неприятно удивлены. Но обязательно сделайте резервную копию системы. Сканер, не разбираясь в сути вопроса, может получить доступ к удаленному управлению, и порядком набедокурить, нажимая на все доступные кнопки.

6. Серьезно относитесь к настройке рабочей станции, с которой происходит управление системой. Сам автор использует следующий подход, легко реализуемый с помощью настройки Proxy-сервера:

   - бразуер, использующийся для работы в корпоративной сети не имеет доступа к ресурсам Internet.

- браузер, работающий с Internet ограничен в использовании корпоративных ресурсов и работает в "песочнице".

7. Дополнительно можно заблокировать выполнение сценариев в зоне безопасности My Computer [12].

Попытайтесь относиться к системе WIDS как к критичному бизнес-приложению, и выполнить сформулированные в политике безопасности требования для данного класса продуктов. Кроме внеочередного пересмотра политики вы получите уникальную возможность побывать на месте специалистов ИТ и пользователей, ежедневно выполняющих(?) требования политики.

Об авторе

Сергей Гордейчик работает системным архитектором компании Positive Technologies (www.ptsecurity.ru), где он специализируется в вопросах безопасность приложений, безопасности беспроводных и мобильных технологий. Автор также является ведущим разработчиком курсов "Безопасность беспроводных сетей", "Анализ и оценка защищенности Web-приложений" учебного центра «Информзащита» (www.itsecurity.ru). Опубликовал несколько десятков статей в "Windows IT Pro/RE", SecurityLab (www.securityfocus.ru) и других изданиях. Является участником Web Application Security Consortium (WASC).

О компании Positive Technologies

Основное направление деятельности компании — защита компьютерных сетей от несанкционированного доступа. Говоря проще, мы помогаем нашим клиентам защититься от хакеров и других непрошенных виртуальных гостей.

Свою основную задачу мы решаем тремя путями:

- предоставляем услуги по аудиту и защите вычислительных сетей, серверов, рабочих станций;
- развиваем один из лучших в мире сканеров безопасности XSpider, который клиент может использовать самостоятельно для поиска и устранения уязвимостей;
- обеспечиваем информационную поддержку профессионалам на страницах принадлежащего нам ведущего российского портала по информационной безопасности securitylab.ru.

Являясь специализированной компанией, мы способны обеспечить самый высокий уровень сервиса в своей области. В то же время, имея богатый и успешный опыт работы в сфере информационных технологий, мы по желанию клиента готовы предоставить и более комплексные решения (начиная от проектирования архитектуры локальной сети, поставки оборудования и кончая поддержкой и сопровождением всей сетевой программно-аппаратной инфраструктуры).

Ссылки

[1] Vulnerabilities in Snort 2.4
http://www.security.nnov.ru/soft/6810.html?l=EN
[2] Kevin Finisterre, «New Kismet Packages available - SayText() and suid kismet_server issues»
http://www.security.nnov.ru/docs3012.html
[3] Johnny «Cache», David Maynor «Device Drivers: Dont build a house on a shaky foundation»
www.blackhat.com/presentations/bh-usa-06/BH-US-06-Cache.pdf
[4] AirMagnet Enterprise
http://www.airmagnet.com/products/enterprise.htm
[5] «SPI Dynamics WebInspect Cross Application Script Injection Vulnerability»
http://www.securityfocus.com/bid/14385/references
[6] SPI Dynamics, «Feed Injection in Web 2.0»
http://www.spidynamics.com/assets/documents/HackingFeeds.pdf
[7] Joshua Wright, «Weaknesses in Wireless LAN Session Containment»
http://i.cmpnet.com/nc/1612/graphics/SessionContainment_file.pdf
[8] Web Application Security Consortium, Threats Classification
http://www.webappsec.org/projects/threat/
[9] Cisco Security Advisory: Multiple Vulnerabilities in the WLSE Appliance
http://www.cisco.com/warp/public/707/cisco-sa-20060419-wlse.shtml
[10] Cain & Abel
http://www.oxid.it/cain.html
[11] Raw Wireless Tools Homepage
http://rfakeap.tuxfamily.org/
[12] How to strengthen the security settings for the Local Machine zone in Internet Explorer
http://support.microsoft.com/kb/833633