К. В. Савик

МЕТОДЫ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ

Сетевая безопасность состоит из аппаратных и программных компонентов, предназначенных для защиты данных и информации, обрабатываемой в сети. Кроме того, эти компоненты обеспечивают установку профилактических мер для защиты сетевой инфраструктуры и ее данных от несанкционированного доступа, изменения данных, повреждения и несанкционированного раскрытия. В конечном счете, сетевая безопасность предназначена для создания безопасной среды, в которой пользователи компьютеров, программ и мобильных приложений могут выполнять компьютерные или цифровые действия без сетевых уязвимостей.

Введение

Надежность и безопасность сети крайне важны в мире, где компьютерные сети являются ключевым элементом в коммуникациях и транзакциях между объектами. Сетевые администраторы, правительство, консультанты по безопасности и хакеры использовали различные инструменты для проверки уязвимостей целевых сетей, таких как, например, возможность удаленного доступа к компьютерам в сети и управления ими без авторизации. Благодаря этому интенсивному тестированию целевая сеть может быть «защищена» от распространенных уязвимостей и эзотерических атак. Однако существующие системы тестирования дают противоречивые результаты, используют недоказанные методы или наносят ущерб целевой сети.

Таким образом, целью данной работы является исследование методов обнаружения уязвимостей в распределенных системах на примере ARP-spoofing (ARP - poisoning).

I. ARP-spoofing

ARP-spoofing (ARP-poisoning) — техника сетевой атаки, применяемая преимущественно в Ethernet, но возможная и в других, использующих протокол ARP сетях, основанная на использовании недостатков протокола ARP и позволяющая перехватывать трафик между узлами, которые расположены в пределах одного широковещательного домена [1]. Относится к числу spoofing-атак.

До выполнения ARP-spoofing'а в ARP-таблице узлов A и B существуют записи с IP- и MAC-адресами друг друга. Обмен информацией производится непосредственно между узлами A и B.

В ходе выполнения ARP-spoofing'а компьютер (Hacker), выполняющий атаку, отправляет ARP-ответы (без получения запросов):

- узлу A: с IP-адресом узла B и MAC-адресом узла Hacker;
- узлу B: с IP-адресом узла A и MAC-адресом узла Hacker.

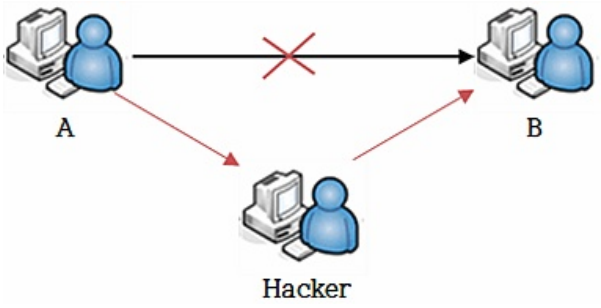

Рис. 1 – ARP-spoofing в локальной сети

В силу того что компьютеры поддерживают самопроизвольный ARP (gratuitous ARP), они модифицируют собственные ARP-таблицы и помещают туда записи, где вместо настоящих MAC-адресов компьютеров A и B стоит MAC-адрес компьютера Hacker.

После того как атака выполнена, когда компьютер A хочет передать пакет компьютеру B, он находит в ARP-таблице запись (она соответствует компьютеру Hacker) и определяет из неё MAC-адрес получателя. Отправленный по этому MAC-адресу пакет приходит компьютеру Hacker вместо получателя. Компьютер Hacker затем ретранслирует пакет тому, кому он действительно адресован — т.е. компьютеру B.

II. Методы обнаружения

Программа arpwatch отслеживает всю ARP-активность на указанных интерфейсах. arpwatch — демон, который отслеживает соответствие между IP и MAC-адресами, и при обнаружении аномалий, сообщающий об этом в Syslog. Используется как один из инструментов для борьбы с ARP-spoofing'ом.

Демон анализирует ARP-ответы на сетевом интерфейсе, к которому он привязан, и запоминает соответствие IP-адресов и MAC-адресов. Как только он видит, что соответствие нарушено, или обнаруживает появление новых адресов в сети, он сообщает об этом в системный журнал (syslog).

Если коммутатор управляемый, можно определить, на каком из его портов работает узел, имеющий определённый MAC-адрес.

Например, это можно сделать с помощью скрипта mac2port [2]. Скрипт связывается с коммутатором по SNMP и опрашивает его таблицу соответствия MAC-адресов портам. Полученная информация выдаётся в удобном для поиска виде на стандартный поток вывода. Условия для использования скрипта:

- скрипт должен быть размещён в каталоге /usr/local/bin, или другом каталоге указанном в PATH;
- скрипт должен быть исполняемым (chmod +x mac2port);
- в теле скрипта должен быть указан IP-адрес коммутатора и его SNMP RO community;
- коммутатор должен поддерживать SNMP версии 2.

III. Методы предотвращения

Борьба с ARP-spoofing'ом с помощью arpwatch оказывается простой, но не эффективной.

- для того чтобы зафиксировать атаку, на защищаемых узлах должна работать программа arpwatch (или аналогичная);
- arpwatch позволяет только зафиксировать атаку, но он не в состоянии её предотвратить.

Одним из решением может быть статический ARP [4], т.е. отказаться от использования ARP протокола. В этом случае необходимо сформировать ARP-таблицу в ручную. Для этого надо добавить MAC-адресв в таблицу, таким образом она становится неуязвима к ARP-атакам. Недостатками такого подхода будет то, что каждое изменение в сети, связанное с заменой или перестановкой сетевых карт, должно сопровождаться редактирование ARP-таблиц в файлах. Так же клиентские узлы все еще уязвимы для ARP-spoofing'a.

Еще одним решением являются патчи ядра системы [3]. Суть метода состоит в том, что при приеме ARP-ответа производится сравнение старого и нового MAC-адресов, и при обнаружении его изменения запускается процедура верификации. Посылается ARP-запрос, требующий всем хозяевам IP-адреса сообщить свои MAC-адреса.

Использование VLAN. Компьютер Hacker может использовать ARP-spoofing против компьютера A только в том случае, если они находятся в одной сети канального уровня. В том случае, если они разделены маршрутизатором, атака возможна только на маршрутизатор. VLAN'ы помогают сегментировать сеть - превратить одну сеть в множество изолированных на канальном уровне фрагментов, которые соединены между собой маршрутизатором. Атака ARP- spoofing возможна только между компьютерами находящимися в одном VLAN'е. В наиболее крайнем случае, когда в каждом VLAN'е находится только два компьютера: собственно компьютер и маршрутизатор, атака ARP-spoofing становится невозможной в принципе. К сожалению, такая организация сети являются очень требовательной к ресурсам маршрутизатора и используется редко.

IV. Вывод

В ходе проведенной работы был проведен обзор атаки ARP-spoofing, проведение данной атаки, методы обнаружения и методы предотвращения. Исходя из проведенной работы, стало видно, что ARP протокол небезопасен и имеет ряд проблем, например, он не обладает никакими способами проверки поблинности пакетов (запросов и ответов). Используя его уязвимости можно получить доступ к исходящему трафику пользователя. Из этого следует то, что есть необходимость для обнаружения и предотвращения атак подобного типа.

1. Ramachandran V., Nandi S. Detecting ARP spoofing: An active technique //International Conference on Information Systems Security. – Springer, Berlin, Heidelberg, 2005. – С. 239-250.
2. http://xgu.ru/downloads/mac2port
3. https://www.securitylab.ru/analytics/216229.php
4. Kwon K., Ahn S., Chung J. W. Network security management using ARP spoofing //International Conference on Computational Science and Its Applications. – Springer, Berlin, Heidelberg, 2004. – С. 142-149.

Савик Константин Викторович, магистрант 1 курса факультета информационных технологий и управления Белорусского государственного университета информатики и радиоэлекстроники, hootkich@gmail.com.

Научный руководитель: Захарьев Вадим Анатольевич, доцент кафедры систем управления Белорусского государственного университета, кандидат технических наук, zahariev@bsuir.by.