МАРШРУТИЗАТОР ИЛИ ПОТАЙНАЯ ДВЕРЬ К ДАННЫМ

Ильинов Д.В.[1], Шмакова Е.Г.[2]

[1]Ильинов Денис Владимирович - студент магистратуры;
[2]Шмакова Елена Германовна – кандидат технических наук, доцент,
кафедра информационных систем, сетей и безопасности,
Российский государственный социальный университет,
г. Москва

Аннотация: *целью работы в данной статье является предложение по предупреждению компрометации коммутирующих устройств (маршрутизаторов, коммутаторов) в домашних условиях. Цели достигнуты путем решения следующих задач: проведен анализ существующих методов нанесения ущерба коммутирующим устройствам; проведен анализ решений и выделены преимущества в найденных решениях; разработана структурная схема с сегментами домашней подсети; проведен автоматизированный анализ сети; проанализированы уязвимости исследуемой подсети; предложено устранение уязвимостей. Современность и актуальность проделанной работы в статье заключаются в том, что в мире идет беспрерывное информационное противоборство, из-за которого персональные данные и личная информация могут быть использованы со злым умыслом против собственника данной информации.*

Ключевые слова: *маршрутизатор, коммутатор, компрометация данных, взлом маршрутизатора, анализ трафика.*

В качестве примера была рассмотрена транснациональная корпорация Cisco Systems.

Cisco Systems — американская транснациональная компания, разрабатывающая и продающая коммутационное оборудование. Стремится представить полный спектр сетевого оборудования, и таким образом предоставить возможность клиенту закупить абсолютно всё необходимое сетевое оборудование исключительно у себя.

Сетевая компания внедрила многоуровневую разветвлённую систему сертификации специалистов по IT технологиям. Благодаря тому, что экзамены этой системы проверяют наличие знаний продукции, а также знание сетевых технологий и протоколов, немалое количество организаций признают ценность профессиональных сертификатов выше представленной компании. Непосредственно, сертификация на уровне эксперта (CCIE) является одной из самых известных и авторитетных в компьютерной индустрии.

По состоянию на начало 2016 года Cisco производит большое количество аппаратно-программных средств, от коммутаторов до крупных систем видеовещания, но и это не мешает столь крупной компании совершать ошибки в функционировании оборудования и, непосредственно, внутренних технологий и протоколов [2].

Факты о некомпетентности Cisco systems в среде информационной безопасности: группа быстрого реагирования на компьютерные инциденты (US-CERT) опубликовала информационный список в начале осени 2014 года, в котором предупредила об обнаружении уязвимости в приложении для удаленного управления серверами Integrated Management Controller (IMC) от Cisco. IMC — это контроллер управления материнской платой, позволяющий контролировать за всеми встроенными сервисами на многоуровневых-серверах (blade) UCS E-Series производства Cisco. Уязвимость была найдена в SSH-модуле IMC, она открывает возможность для удаленного вывода сервера из строя. «Данная уязвимость существует из-за нестабильной обработки контроллером специально сформированных SSH-пакетов», — отметила Cisco в своем официальном заявлении. Отправляя специально сформированные пакеты на SSH-сервер, управляемый через IMC, хакеры могут вызвать отказ в обслуживании. На операционную систему многоуровневого-сервера подобная атака воздействие не оказывает, как заявили в Cisco. Проверку сетевых устройств на наличие утечек информации злоумышленники обычно осуществляют с помощью генератора специальных пакетов и не используют регулярный сетевой трафик.

«Успешная эксплуатация уязвимости может остановить работу контроллера Cisco IMC на подверженном атаке многоуровневом-сервере, — отметила Cisco в своем сообщении.

На тему безопасности встроенных контроллеров управления материнской платой был проведен ряд дополнительных исследований. Такие известные эксперты, как разработчик SATAN Дэн Фармер (Dan Farmer) и создатель Metasploit Х.Д. Мур (HD Moore), указали на множество проблем данных контроллеров, в том числе ненадежный или дефектный способ аутентификации, повышающий риск несанкционированного доступа к сетевому устройству. Вопрос о проблемах в BMC был поднят более года назад, когда Фармер обнаружил более пяти критических уязвимостей, включая возможность обхода аутентификации, а также бреши в UPnP, которые могут привести к компрометации прав привилегированного пользователя. Мур сотрудничал с Фармером при проведении тестового интернет-

сканирования IPMI — протокола, использующегося в большинстве BMC-контроллеров. В результате исследования эксперты пришли к выводу, что уязвимостям подвержены сотни тысяч серверов и прочих сетевых устройств: у части из них отсутствует шифрование, другие же имеют проблемы с аутентификацией [3].

Что говорить о домашней сети, а тем более о ее безопасности, когда корпорации гиганты не могут обеспечить сего, хотя там проблемой безопасности занимаются целые подразделения.

Чтобы доказать компетентность предположений, был проведен опыт, который доказывает, что безопасность сетевых технологий понятие абстрактное. В качестве взламываемого протокола был выбран WPA/WPA2, так как он является наиболее защищенным, по словам компаний производителей маршрутизаторов и СМИ. Название ПО решено оставить скрытым.

В ходе опыта была запущена виртуальная машина «ПРОГРАММЫ ДЛЯ ВЗЛОМА», скачанную из общедоступного сайта при помощи ПО VMware player' a [4].

Запуск и прогон ПО представлен на рисунках 1-6.

Рис. 1. Создание виртуальной машины

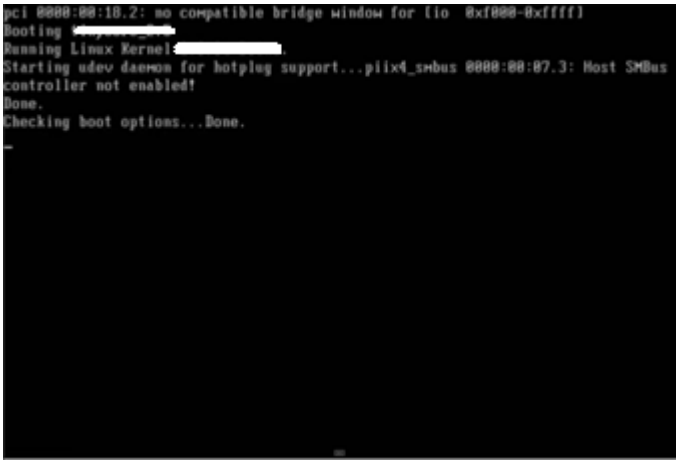

Рис. 2. Загрузка «Программы для взлома»

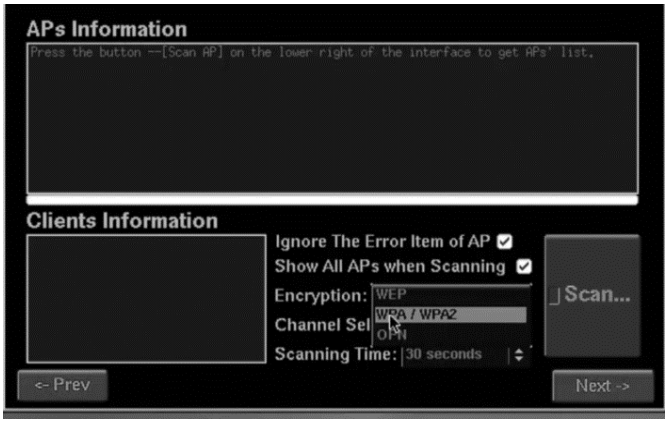

Рис. 3. Выбор варианта взламываемого шифрования

Рис. 4. Подмена MAC-адреса маршрутизатора

Рис. 5. Подбор пароля маршрутизатора, встроенным модулем “Bruteforce”

Рис. 6. Результат подбора

В итоге, был получен пароль от маршрутизатора, что и являлось целью.

Взлом Wi-Fi маршрутизатора можно обнаружить по некоторым общим признакам. В первую очередь Вы заметите, что скорость доступа регулярно снижается. Это может быть вызвано различными проблемами – от загруженности канала до взлома вашего маршрутизатора, поэтому, Вам также следует визуально проверить, как интенсивно используется Ваш маршрутизатор: при обмене информацией индикатор WAN на маршрутизаторе светится. Если Вы точно знаете, что все устройства выключены, а этот индикатор мигает, то возможно кто-то подключен к Вашему маршрутизатору. Этот метод не всегда корректен, так как индикаторы на разных маршрутизаторах могут работать по-разному и даже мерцать при отключенных устройствах, поэтому Вам следует зайти в пользовательский интерфейс маршрутизатора, зайдя в браузер и перейдя по IP адресу маршрутизатора (стандартный 192.168.1.1) и

проверить перечень подключенных устройств. По названиям в списке подключенных устройств, Вы сможете определить чужие устройства, и отключить их [1].

Необходимо усвоить минимальный набор правил, представленных ниже, чтобы обезопасить Ваш маршрутизатор от взлома.

Каждый маршрутизатор имеет свой IP адрес в сети. По умолчанию, IP адресом маршрутизатора является адрес 192.168.1.1. Этот IP адрес используется для того, чтобы подключаться к пользовательскому интерфейсу маршрутизатора, с помощью которого можно управлять всеми настройками маршрутизатора. Но, при вводе IP адреса мы не попадаем сразу в пользовательский интерфейс, так как он имеет логин и пароль, которые требуется ввести. Обычно, стандартные логин и пароль – admin/admin. Исходя из описанного, можно сделать вывод, что, находясь в открытой сети, злоумышленник, имеет возможность ввести стандартные IP адрес, а также логин и пароль, и завладеть управлением нашего маршрутизатора. Чтобы этого не допустить, в настройках маршрутизатора необходимо поменять стандартный IP адрес маршрутизатора, а также логин и пароль на персональные.

По аналитическим данным, приводимым компанией Tripwire:

- 46% рядовых пользователей не изменяют установленный в маршрутизаторе по умолчанию пароль администратора.
- 80% из топ-25 самых продаваемых в интернет-магазине Amazon моделей уязвимы для хакерских атак.
- 34% этих незащищенных устройств подвержены еще большей угрозе компрометации, поскольку в открытом доступе опубликован код соответствующих эксплоитов*, ориентированных на конкретную модель и версию прошивки.

Также, для усложнения доступа к вашей Wi-Fi сети, Вам следует сконфигурировать сложный пароль (с разными регистрами, языками, цифрами), с защитой WPA2 (она считается лучшим выбором, чем WEP, так как вышла позднее, хотя в опыте, приводимом нами выше, WPA2 взламывается довольно несложно), так же нужно поменять название сети со стандартного на свое, и скрыть название сети, для того, чтобы при входе в вашу сеть, следовало вводить не только пароль, но и название сети. Поиск скрытой сети немного усложнит задачу злоумышленнику, а сложный пароль заставит его тратить много времени для взлома.

Выше представленная информация говорит нам о том, что ничто не может гарантировать 100% безопасность. Даже если взять лицензионный антивирус с полностью обновленными базами, который защищает на 99%, как указано в паспорте продукта, то мы получаем: По приведенной статистике за 2013 год было выявлено 3 млн вирусов, т.е. 8219 в день, т.е. 1% составляет 82 вируса, которые теоретически могут заразить ваш ПК.

Только этот факт заставляет задуматься о том, что 100% безопасность может быть обеспечена полным отключением ПК от глобальной сети в домашних условиях, в корпоративных условиях обеспечению информационной безопасности присущи и другие факторы, такие как человеческий фактор, например.

Список литературы

1. Мельников Д.А «Организация и обеспечение безопасности информационно-технологических сетей и систем». М: IDO Press. Университетская книга,– 2012. 598 с.
2. [Электронный ресурс]. Режим доступа: http://www.cisco.com/-Cisco Systems/ (дата обращения: 20.01.2017).
3. [Электронный ресурс]. Режим доступа: http://threatpost.ru/ Сайт публикаций информационных противоборств/(дата обращения: 20.01.2017).
4. [Электронный ресурс]. Режим доступа:http://www.VMware.com/ru Сайт VMware player (справка по работе приложения)/ (дата обращения: 20.01.2017).