Testy penetracyjne sieci – Uzyskiwanie dostępu

Do tej pory nie musieliśmy łączyć się z siecią w żadnym celu. Tu, w ramach nauki testów penetracyjnych sieci, połączymy się z siecią. Pozwoli nam to przeprowadzać silniejsze ataki i uzyskiwać dokładniejsze informacje. Jeśli sieć nie korzysta z szyfrowania (innymi słowy, jeśli jest to otwarta sieć bezprzewodowa), możemy się z nią połączyć i wychwycić niezaszyfrowane dane. Jeśli sieć jest przewodowa, nadal możemy spróbować się z nią połączyć, być może zmieniając adres MAC. Głównym problemem, jaki możemy napotkać, jest sieć korzystająca z szyfrowania (takiego jak WEP, WPA lub WPA2). Jeśli natrafimy na zaszyfrowane dane, musimy znać klucz do ich odszyfrowania – to jest główny cel . Jeśli sieć docelowa korzysta z jakiegoś rodzaju szyfrowania, bez odszyfrowania nie da się niczego osiągnąć. Omówimy, jak odszyfrować szyfrowanie WEP, WPA i WPA2.

Omówione zostaną następujące tematy:

Teoria WEP

Podstawowe łamanie zabezpieczeń sieci

Atak z fałszywym uwierzytelnianiem

Powtórka żądania ARP

Wprowadzenie do WPA

Łamanie zabezpieczeń WPA

Teoria uzgadniania

Przechwytywanie uzgadniania

Tworzenie list słów

Łamanie list słów

Zabezpieczanie sieci przed atakami

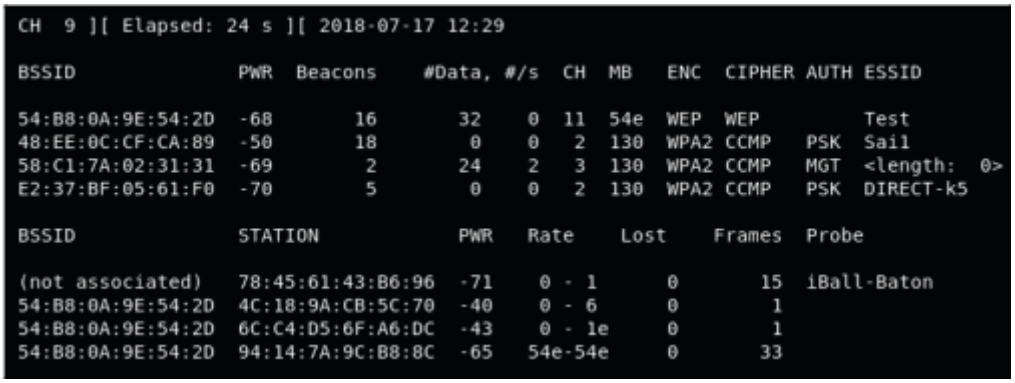
Teoria WEP

Pierwszym szyfrowaniem, które omówimy, jest szyfrowanie Wired Equivalent Privacy (WEP), ponieważ jest ono najstarsze i najłatwiejsze do złamania. Szyfrowanie WEP wykorzystuje algorytm RC4; każdy pakiet jest szyfrowany w punkcie dostępu (AP), a następnie wysyłany w powietrze. Po odebraniu pakietu klient będzie mógł go odszyfrować i odczytać zawarte w nim informacje, ponieważ posiada klucz. Krótko mówiąc, punkt dostępu szyfruje pakiet i wysyła go, a klient odbiera i odszyfrowuje. Analogicznie, gdy klient sam wysyła pakiet, szyfruje go i wysyła, a punkt dostępu odbiera i odszyfrowuje za pomocą klucza. Każdy wysyłany pakiet ma unikalny strumień klucza. WEP zapewnia unikalność strumienia klucza dzięki 24-bitowemu wektorowi inicjalizacji (IV). IV to losowa liczba wysyłana do każdego pakietu w postaci jawnego tekstu, który nie jest zaszyfrowany. Jeśli odczytamy pakiet, będziemy mogli odczytać jego część w postaci zwykłego tekstu. Problem z IV polega na tym, że jest on bardzo krótki (24 bity, co nie jest aż tak długie). W obciążonej sieci zostanie wysłana bardzo duża liczba pakietów, możliwości losowych IV zostaną wyczerpane i ostatecznie otrzymamy dwa pakiety o tym samym IV. W takim przypadku możemy zastosować `aircrack-ng`, który wykorzystuje ataki statystyczne do określenia strumieni kluczy; będzie on w stanie określić klucz WEP. Z powyższych informacji wynika, że im więcej IV zbierzemy, tym większe prawdopodobieństwo, że złamiemy klucz

WEP. Naszym głównym celem, gdy próbujemy złamać szyfr WEP, jest zebranie jak największej liczby identyfikatorów IV – ponieważ przy dużej liczbie identyfikatorów IV otrzymamy dwa pakiety używające tego samego identyfikatora IV, a `aircrack-ng` prawdopodobnie określi strumień klucza i klucz WEP dla sieci docelowej. W następnej części tego rozdziału zobaczymy, jak to właściwie działa i powinno być to łatwiejsze do zrozumienia.

Podstawowe łamanie sieci

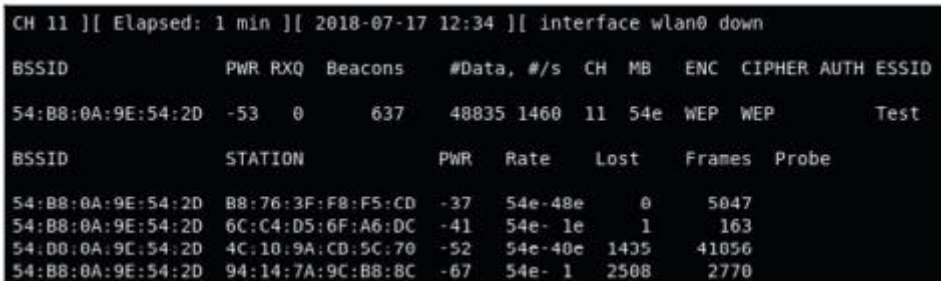
Z poprzedniej sekcji dowiedzieliśmy się, że aby złamać klucz WEP, wystarczy podsłuchiwać pakiety z sieci docelowej i zbierać jak najwięcej identyfikatorów IV. Gdy to zrobimy, `aircrack-ng` będzie mógł użyć ataków statystycznych, aby określić strumień klucza i klucz WEP dla sieci docelowej. Oczywiste jest, że jeśli mamy więcej niż dwa pakiety, metoda będzie skuteczniejsza i ryzyko złamania klucza będzie większe — postaramy się zebrać jak najwięcej IV. Przyjrzyjmy się najprostszemu sposobowi złamania klucza WEP. Karta Wi-Fi musi być w trybie monitorowania, a pierwszą rzeczą, jaką spróbujemy zrobić, jest sprawdzenie wszystkich sieci w zasięgu Wi-Fi; następnie wybierzemy jedną z nich. Uruchomimy `airodump-ng wlan0`, bardzo proste polecenie, gdzie wlan0 oznacza interfejs. Poniżej zostanie wyświetlony następujący komunikat:



Pierwszą siecią, która się pojawiła, jest Test; to właśnie na nią przeprowadzimy ataki. Uruchomimy airodump w sieciTest, używając następującego polecenia:

airodump-ng --bssid 54:B8:0A:9E:54:2D --channel 11 --write basic-test-ap wlan0

W tym miejscu wpisujemy --bssid i uruchamiamy airodump w punkcie dostępowym Test. Dodajemy --channel, numer 11 i dodajemy --write, aby zapisać wszystkie przechwycone pakiety w pliku o nazwie basic-test-up. Po uruchomieniu poprzedniego polecenia będziemy mogli zobaczyć wynik na poniższym zrzucie ekranu. Sieć docelowa, którą mamy, ponieważ zebrane dane są dość obciążone, a dane i ramki są przesyłane:



Sieć jest bardzo zatłoczona. Poniżej znajduje się sekcja, w której możemy zobaczyć klientów:

```
BSSID              STATION            PWR   Rate    Lost    Frames  Probe

54:B8:0A:9E:54:2D  B8:76:3F:F8:F5:CD  -37   54e-48e     0     5047
54:B8:0A:9E:54:2D  6C:C4:D5:6F:A6:DC  -41   54e- 1e     1      163
54:B8:0A:9E:54:2D  4C:18:9A:CB:5C:70  -52   54e-48e  1435    41856
54:B8:0A:9E:54:2D  94:14:7A:9C:B8:8C  -67   54e- 1   2508     2770
```

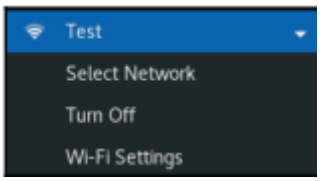
Teraz wystarczy uruchomić `aircrack-ng`, który jest częścią pakietu aircrack, na pliku utworzonym przez airodump. Możemy uruchomić aircrack na tym pliku, nawet jeśli nie zatrzymaliśmy airodump; będzie on kontynuował odczyt pliku i odczytywał nowe pakiety przechwytywane przez airodump. Polecenie, którego należy użyć, wygląda następująco:

aircrack-ng basic-test-ap-01.cap

Kiedy używamy `aircrack-ng`, wpisujemy nazwę pliku basic-test-ap-01.cap . Podczas gdy plik jest tworzony, stając się coraz większy wraz z dołączaniem nowych pakietów, możemy uruchomić `aircrack-ng`, a będzie on stale aktualizowany, ostatecznie podając nam hasło potrzebne do złamania zabezpieczeń. Jeśli aircrack nie uda się ustalić klucza, aircrack czeka, aż osiągnie 5000 IV, a następnie próbuje ponownie. Liczba IV zależy w rzeczywistości od rodzaju szyfrowania WEP. Istnieją dwa rodzaje szyfrowania WEP: 128-bitowe i 64-bitowe. Jedyną różnicą jest długość klucza; oczywiście 64-bitowe wymaga mniejszej liczby IV niż 128-bitowe. Pamiętaj, że kiedy omawialiśmy aircrack, wskazaliśmy, że im więcej pakietów otrzymamy bez unikalnych IV, tym większe są nasze szanse na złamanie klucza WEP. Teraz zasadniczo czekamy, aż aircrack pomyślnie złamie klucz WEP. Po odszyfrowaniu klucza możemy nacisnąć Ctrl + C. Jak widać na poniższym zrzucie ekranu, aircrack pomyślnie uzyskał klucz w pakietach danych. Dzieje się tak, ponieważ docelowy punkt dostępowy używa klucza 64-bitowego:

```
Opening basic-test-ap-01.cap
Read 355742 packets.

   #  BSSID              ESSID                     Encryption

   1  54:B8:0A:9E:54:2D  Test                      WEP (168250 IVs)

Choosing first network as target.

Opening basic-test-ap-01.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 170996 ivs.
                    KEY FOUND! [ 31:31:32:32:39 ] (ASCII: 11229 )
       Decrypted correctly: 100%
```

Zobaczmy, jak możemy użyć tego klucza do połączenia z siecią. Skopiujemy klucz i użyjemy go do połączenia. Następnie możemy połączyć się z siecią docelową:



Jak widać, nasze połączenie zostało nawiązane; udało nam się odzyskać klucz WEP z sieci docelowej. Możemy to potwierdzić, wysyłając ping do Google:

```
root@kali:~# ping www.google.com
PING www.google.com (172.217.160.196) 56(84) bytes of data.
64 bytes from bom07s16-in-f4.1e100.net (172.217.160.196): icmp_seq=1 ttl=56 time=8.33 ms
64 bytes from bom07s16-in-f4.1e100.net (172.217.160.196): icmp_seq=2 ttl=56 time=7.50 ms
64 bytes from bom07s16-in-f4.1e100.net (172.217.160.196): icmp_seq=3 ttl=56 time=7.29 ms
64 bytes from bom07s16-in-f4.1e100.net (172.217.160.196): icmp_seq=4 ttl=56 time=8.24 ms
64 bytes from bom07s16-in-f4.1e100.net (172.217.160.196): icmp_seq=5 ttl=56 time=6.83 ms
64 bytes from bom07s16-in-f4.1e100.net (172.217.160.196): icmp_seq=6 ttl=56 time=6.77 ms
64 bytes from bom07s16-in-f4.1e100.net (172.217.160.196): icmp_seq=7 ttl=56 time=7.67 ms
^C
--- www.google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6025ms
rtt min/avg/max/mdev = 6.773/7.523/8.332/0.570 ms
```

Atak z fałszywym uwierzytelnianiem

W poprzedniej sekcji widzieliśmy, jak łatwo złamać klucz WEP w obciążonej sieci. W obciążonej sieci ilość danych rośnie bardzo szybko. Problem polega na tym, że teraz będziemy symulować punkt dostępowy, do którego nie są podłączeni żadni klienci, lub punkt dostępowy, do którego jest podłączony klient, ale klient nie korzysta z sieci tak intensywnie, jak klient w poprzedniej sekcji (być może klient po prostu czyta artykuły lub korzysta z Facebooka, nie zużywając tak dużo danych, jak widzieliśmy ostatnio). Przyjrzyjmy się przykładowi. Uruchomimy airodump dla docelowego punktu dostępowego, Test, aby przyjrzeć się bezczynnemu punktowi dostępowemu. Mamy teraz Test, ten sam punkt dostępowy, którego używaliśmy wcześniej, ale różnica polega na tym, że odłączyliśmy podłączone urządzenie. Jak widać, w drugim obszarze (obszarze klienta) nie ma podłączonych klientów. Widzimy również, że #Data oznacza 0-, nawet nie dotarło do 1. To będzie problem, z którym przyjdzie nam się zmierzyć – chcemy być w stanie złamać klucz taki jak ten, przy 0 danych:

```
CH 11 ][ Elapsed: 0 s ][ 2018-07-17 13:05

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

54:B8:0A:9E:54:2D  -38 100       50        0    0  11  54e  WEP  WEP         Test

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

Możemy wstrzykiwać pakiety do ruchu. Kiedy wstrzykiwamy pakiety do ruchu, możemy zmusić punkt dostępowy do utworzenia nowych pakietów z nowymi identyfikatorami IV, a następnie przechwycenia tych identyfikatorów. Zanim jednak będziemy mogli wstrzykiwać pakiety, musimy uwierzytelnić nasze urządzenie w docelowym punkcie dostępowym. Punkty dostępowe mają listy wszystkich podłączonych do nich urządzeń i ignorują wszystkie pakiety pochodzące z urządzenia, które nie jest połączone. Jeśli urządzenie nie ma klucza i próbuje wysłać pakiet do routera, router po prostu go zignoruje; nawet nie spróbuje go odczytać ani zobaczyć, co jest w środku. Zanim będziemy mogli wstrzykiwać pakiety do routera, musimy uwierzytelnić się u niego. Użyjemy metody zwanej fałszywym uwierzytelnianiem; jest ona bardzo prosta. Wykonaliśmy już airodump w poprzedniej sekcji. Zobaczmy, jak możemy użyć fałszywego uwierzytelniania. Na poprzednim zrzucie ekranu widzimy, że pod AUTH nie ma żadnej wartości. Po przeprowadzeniu fałszywego uwierzytelnienia zobaczymy tam OPN, co oznacza, że pomyślnie uwierzytelniliśmy nasze urządzenie za pomocą docelowego punktu dostępowego. W tym celu użyjemy następującego polecenia:

aireplay-ng --fakeauth 0 -a 54:B8:0A:9E:54:2D -h 2e:a0:66:4b:85:29 wlan0

W przypadku `aireplay-ng` zastosujemy atak --fakeauth; uwzględniamy typ ataku i liczbę pakietów, które chcemy wysłać, czyli –fakeauth 0. Umieścimy po prostu 0; niektórzy używają dużej liczby, gdy przeprowadzają atak, który potrwa 5 lub 10 minut, ale my po prostu użyjemy 0, i być może zmienimy to później. Użyjemy opcji -a i docelowego adresu MAC (czyli `54:B8:0A:9E:54:2D`). Następnie

użyjemy -h, aby uwzględnić nasz adres MAC, tak aby nasz adres MAC został uwierzytelniony w sieci docelowej. Aby uzyskać adres MAC, uruchomimy polecenie `ifconfig wlan0`:

```
root@kali:~# ifconfig wlan0
wlan0: flags=803<UP,BROADCAST,NOTRAILERS,PROMISC,ALLMULTI>  mtu 1500
        ether 2e:a0:66:4b:85:29  txqueuelen 1000  (Ethernet)
        RX packets 106326  bytes 45306410 (43.2 MiB)
        RX errors 0  dropped 54113  overruns 0  frame 0
        TX packets 29  bytes 3408 (3.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Nazwa naszej karty Wi-Fi to wlan0. Za pomocą `aireplay-ng`, czyli rodzaju ataku, który próbujemy przeprowadzić, próbujemy przeprowadzić atak fałszywego uwierzytelnienia, aby uwierzytelnić nasz adres MAC, abyśmy mogli wstrzykiwać pakiety do sieci docelowej. Wyślemy 0 (co oznacza „zrób to raz"), następnie -a (z adresem MAC punktu dostępowego), następnie -h (gdzie wpisujemy adres MAC urządzenia, dla którego chcemy przeprowadzić fałszywe uwierzytelnienie), a następnie wlan0, nazwę karty Wi-Fi; teraz naciskamy Enter:

```
root@kali:~# aireplay-ng --fakeauth 0 -a 54:B8:0A:9E:54:2D -h 2e:a0:66:4b
:85:29 wlan0
13:22:06  Waiting for beacon frame (BSSID: 54:B8:0A:9E:54:2D) on channel
11

13:22:06  Sending Authentication Request (Open System) [ACK]
13:22:06  Authentication successful
13:22:06  Sending Association Request [ACK]
13:22:06  Association successful :-) (AID: 1)
```

Jak widać na poprzednim zrzucie ekranu, -a wysłał żądanie uwierzytelnienia i zostało ono pomyślnie wykonane. Sieć stała się siecią otwartą, a nasz klient (czyli moje urządzenie atakujące) wyświetlał się tak, jakby był klientem podłączonym do sieci. W rzeczywistości nie jesteśmy połączeni, ale jesteśmy uwierzytelnieni w sieci i mamy z nią powiązanie, dzięki czemu możemy wstrzykiwać pakiety do punktu dostępowego – będzie on teraz odbierał każde żądanie, które do niego wyślemy. Poniżej znajduje się wynik:

```
CH 11 ][ Elapsed: 36 s ][ 2018-07-17 13:22

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

54:B8:0A:9E:54:2D  -40  92      395       32    0  11  54e  WEP  WEP    OPN  Test

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

54:B8:0A:9E:54:2D  2E:A0:66:4B:85:29    0   54 - 1      0       36
```

W następnej sekcji pokażemy, jak wstrzykiwać pakiety i jak bardzo szybko zwiększyć ilość danych.

Odtwarzanie żądania ARP

Punkt dostępowy akceptuje teraz wysyłane przez nas pakiety, ponieważ nie będzie nas ignorował, skoro udało nam się z nim pomyślnie połączyć za pomocą ataku z fałszywym uwierzytelnianiem. Jesteśmy teraz gotowi do wstrzykiwania pakietów do punktu dostępowego i bardzo szybkiego zwiększania ilości danych, aby odszyfrować klucz WEP. Pierwszą metodą wstrzykiwania pakietów, o której będziemy mówić, jest odtwarzanie żądania ARP. W tej metodzie będziemy czekać na pakiet ARP, przechwytywać go i wstrzykiwać do ruchu. Kiedy to zrobimy, punkt dostępowy będzie zmuszony utworzyć nowy pakiet z nowym identyfikatorem IV; przechwycimy nowy pakiet, ponownie wstrzykniemy go do ruchu i zmusimy punkt dostępowy do utworzenia kolejnego pakietu z kolejnym identyfikatorem IV. Będziemy to powtarzać, aż ilość danych będzie wystarczająco duża, aby złamać

klucz WEP. Zróbmy to w systemie Kali Linux. Pierwszą rzeczą, którą zrobimy, będzie uruchomienie `airodump-ng` za pomocą następującego polecenia:

airodump-ng --bssid 54:B8:0A:9E:54:2D --channel 11 --write arp-request-repl-test wlan0

Dodamy opcję --write do polecenia; nazwijmy ją arp-request-reply-test. Po uruchomieniu zobaczymy, że sieć docelowa ma dane, nie ma powiązanych z nią klientów i nie ma ruchu, ponieważ żaden klient nie jest połączony, co oznacza, że jest bezużyteczna; nie możemy złamać jej klucza. Pierwszą rzeczą, którą zrobimy, będzie atak z fałszywym uwierzytelnieniem, jak pokazano w sekcji „Fałszywe uwierzytelnianie", dzięki czemu będziemy mogli rozpocząć wstrzykiwanie pakietów do sieci, które zostaną zaakceptowane. To prowadzi nas do kolejnego kroku, czyli kroku żądania-odpowiedzi ARP, w którym będziemy wstrzykiwać pakiety do sieci docelowej, wymuszając na niej tworzenie nowych pakietów z nowymi identyfikatorami IV. Polecenie będzie wyglądać następująco:

aireplay-ng --arpreplay -b 54:B8:0A:9E:54:2D -h be:03:87:39:5e:5a wlan0

Jest ono bardzo podobne do poprzedniego polecenia, ale zamiast --fakeauth, użyjemy --arpreply. Dodamy również -b, dla BSSID. Za pomocą tego polecenia będziemy czekać na pakiet ARP, przechwycić go, a następnie ponownie wysłać w powietrze. Wtedy zobaczymy, że przechwyciliśmy pakiet ARP, wstrzyknęliśmy go, przechwyciliśmy kolejny, wstrzyknęliśmy go do ruchu i tak dalej; Następnie AP tworzy nowe pakiety z nowymi IV, odbieramy je, wstrzykujemy je ponownie i tak w kółko:

```
root@kali:~# aireplay-ng  --arpreplay -b 54:B8:0A:9E:54:2D -h be:03:87:39:5e:5a
wlan0
13:58:35  Waiting for beacon frame (BSSID: 54:B8:0A:9E:54:2D) on channel 11
Saving ARP requests in replay_arp-0717-135835.cap
You should also start airodump-ng to capture replies.
Read 1032 packets (got 4 ARP requests and 118 ACKs), sent 146 packets...(337 pps
Read 1073 packets (got 4 ARP requests and 132 ACKs), sent 172 packets...(323 pps
Read 1145 packets (got 4 ARP requests and 168 ACKs), sent 226 packets...(354 pps
Read 1200 packets (got 4 ARP requests and 200 ACKs), sent 260 packets...(352 pps
```

Gdy liczba Data osiągnie 9000 lub więcej, możemy uruchomić aircrack-ng. Gdy użyjemy aircrack-ng i nazwy pliku, z pewnością zobaczymy klucz WEP i będziemy mogli go złamać po 15012 IV:

```
              [00:06:09] Tested 6684673 keys (got 15012 IVs)

KB    depth   byte(vote)
 0    0/  1   4B(21760) 37(20224) 51(20224) EB(20224) 1F(19712)
 1    0/  1   17(21248) CE(20736) 92(20480) 03(20224) 85(19968)
 2    0/  1   80(22784) 06(20992) 27(20480) 94(20480) 05(19968)
 3    0/  1   E4(24832) 0E(20736) 02(19712) 40(19712) F2(19200)
 4    0/  1   E2(22016) 39(20736) 57(20736) F0(20736) 4D(20480)
 5    0/  1   05(22016) 3E(20224) D9(20224) 46(19968) B5(19968)
 6    0/  1   20(20992) 9C(19712) 9F(19712) 04(19456) 3F(19456)
 7    0/  2   86(20992) 62(20736) F5(19968) 79(19712) 1D(19456)
 8    2/  8   C2(19200) 3F(18688) 95(18688) CF(18688) 0A(18432)
 9    0/  1   6F(22528) 12(21760) 1A(21248) 70(20480) 71(19712)
10    0/  1   15(20224) 92(20224) 5C(19968) B2(19968) F7(19968)
11    0/  1   42(22272) 69(21504) 70(20224) BE(19712) 16(19456)
12    0/ 12   43(19828) 3F(19052) 28(18960) 6C(18916) C2(18744)

                KEY FOUND! [ 31:31:32:32:35 ] (ASCII: 11225 )
     Decrypted correctly: 100%
```

Wprowadzenie do WPA

W kolejnych częściach omówimy szyfrowanie Wi-Fi Protected Access (WPA). Szyfrowanie to zostało opracowane po WEP, aby rozwiązać wszystkie problemy, które sprawiały, że WEP było bardzo łatwe do złamania. Głównym problemem z WEP jest krótki IV, który jest wysyłany w każdym pakiecie jako zwykły tekst. Krótki IV oznacza, że możliwość posiadania unikalnego IV w każdym pakiecie może zostać wyczerpana w aktywnych sieciach, co oznacza, że podczas wstrzykiwania pakietów (lub w naturalnych,

aktywnych sieciach) otrzymamy więcej niż jeden pakiet z tym samym IV. W takim przypadku aircrack-ng może wykorzystać ataki statystyczne do określenia strumienia klucza i klucza WEP dla danej sieci. W WPA jednak każdy pakiet jest szyfrowany za pomocą unikalnego, tymczasowego klucza. Oznacza to, że liczba zebranych pakietów danych nie ma znaczenia; nawet jeśli uda nam się zebrać milion pakietów, pakiety te nie będą przydatne, ponieważ nie zawierają żadnych informacji, które mogłyby pomóc nam złamać klucz WPA. WPA2 działa tak samo; działa tą samą metodą i można je złamać tą samą metodą. Jedyną różnicą między WPA a WPA2 jest to, że WPA2 wykorzystuje do szyfrowania algorytm o nazwie Counter-Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP).

Łamanie WPS

Łamanie szyfrowanych sieci WPA lub WPA2 nie jest proste, zwłaszcza że wszystkie wysyłane pakiety są dla nas bezużyteczne, ponieważ nie zawierają żadnych informacji, które mogłyby pomóc nam w ustaleniu klucza WPA. Zanim przejdziemy do łamania WPA i WPA2, przyjrzymy się funkcji o nazwie WPS; pozwala ona użytkownikom i klientom na łączenie się z siecią za naciśnięciem jednego przycisku. W systemie Windows 8, jeśli spojrzysz na niektóre drukarki Wi-Fi, zobaczysz przycisk WPS. Jeśli naciśniesz przycisk WPS i przejdziesz do routera, naciskając również przycisk WPS, lub jeśli przejdziesz do strony konfiguracji i naciśniesz przycisk WPS, klient, drukarka lub urządzenie z systemem Windows połączy się z siecią bez konieczności ręcznego wprowadzania klucza. WPS to funkcja, która umożliwia klientom łatwe łączenie się z siecią, bez konieczności ręcznego wprowadzania klucza WPA; to tylko funkcja routerów. Ta funkcja uwierzytelnia klienta za pomocą 8-cyfrowego kodu PIN, nie używa faktycznego klucza WPA. WPS składa się tylko z cyfr, więc nie ma zbyt wielu możliwości. Jeśli zastosujemy atak siłowy, z pewnością odgadniemy kod PIN. Jeśli odgadniemy kod PIN, możemy użyć narzędzia o nazwie Reaver, które obliczy klucz WPA na podstawie kodu PIN. Zamierzamy złamać kod PIN metodą siłową; ponieważ ma on tylko 9 cyfr, odniesiemy sukces. Po wykonaniu tej czynności możemy obliczyć klucz WPA za pomocą Reavera. Aby wyszukać punkty dostępowe z włączonym WPS, użyjemy narzędzia Wash. Użyjemy polecenia Wash -i wlan0. Na poniższym zrzucie ekranu widzimy nasz testowy punkt dostępowy – to ten punkt dostępowy, który zamierzamy złamać. Działa on teraz w trybie WPA, a nie WEP, jak widzieliśmy wcześniej:

```
root@kali:~# wash -i wlan0
BSSID              Ch  dBm  WPS  Lck  Vendor    ESSID
--------------------------------------------------------------------
48:EE:0C:CF:CA:89   1  -66  2.0  No   RalinkTe  Sail
E2:37:BF:05:61:F0   1  -74  2.0  No             DIRECT-k5
54:B8:0A:9E:54:2D  11  -59  2.0  No   RealtekS  Test
```

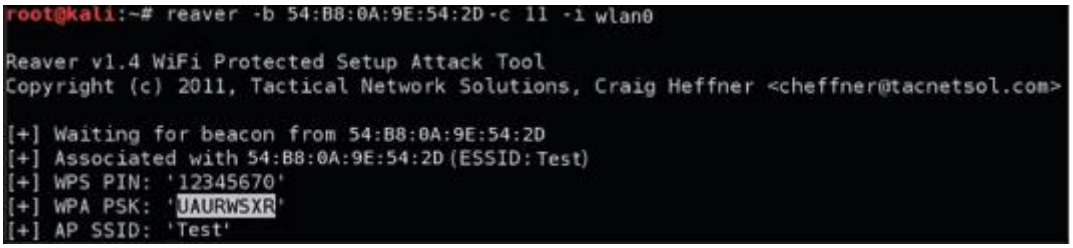
Aby sprawdzić, czy punkt dostępowy rzeczywiście używa szyfrowania WPA, uruchom polecenie `airodump-ng wlan0`.

Powyżej znajduje się lista punktów dostępowych z włączonym WPS. Możemy zobaczyć Ch, dBm (który oznacza odległość między nami a punktem dostępowym), WPS oznaczającą wersję WPS oraz Lck oznaczającą, czy jest zablokowany. Niektóre routery, gdy próbujemy wymusić kod PIN WPS metodą brute force, blokują się po kilku nieudanych próbach. Jeśli na przykład spróbujemy podać cztery błędne kody PIN, zostaną zablokowane i nie będą akceptować żadnych kodów PIN przez określony czas. Jeśli Lck wyświetla Yes, nie możemy już przeprowadzić ataku; musimy poczekać chwilę, a następnie wrócić do punktu dostępowego. Uruchomimy teraz reaver, który wymusi włamanie się na kod PIN WPS, a po jego znalezieniu wyliczy klucz WPA. reaver obsługuje wstrzymywanie i wznawianie, na przykład, jeśli za pomocą wymuszenia osiągniemy 30% możliwości, a następnie anulujemy atak, po powrocie zaczniemy od 30, a nie od 0. Uruchommy reavwer; Wpiszemy -b, aby wybrać BSSID, czyli adres MAC,

docelowego punktu dostępowego, a następnie -c, aby wybrać kanał, który wynosi 11. Następnie możemy wybrać kartę Wi-Fi -i w trybie monitorowania, czyli wlan0. Polecenie wygląda następująco:

reaver -b 54:B8:0A:9E:54:2D -c 11 -i wlan0

Naciskamy Enter, a reaver zostanie skojarzony z docelowym punktem dostępowym; spróbuje on ustalić kod PIN WPS. Na zrzucie ekranu widać, że mamy prosty kod PIN, który wynosi 12345670; na tej podstawie reaver był w stanie obliczyć klucz WPA, UAURWSXR:



Teraz możemy połączyć się z siecią; jeśli wprowadzimy klucz, który właśnie znaleźliśmy, możemy użyć hasła UAURWSXR i nawiązać połączenie.

Teraz mamy kilka opcji dla reaver. Uruchamiamy reaver --help i widzimy wszystkie opcje, których możemy użyć z reaver. Jak wspomniano wcześniej, niektóre routery blokują się po kilku nieudanych próbach; dlatego możemy użyć niektórych z tych zaawansowanych opcji reaver, aby działał przeciwko tym punktom dostępowym. Na przykład, możemy użyć opcji --delay, aby określić czas (w sekundach), jaki reaver powinien odczekać między każdą próbą ataku siłowego lub każdą próbą wprowadzenia kodu PIN. Możemy również użyć opcji –lock -delay, aby nakazać reaver odczekać np. 60 sekund, jeśli AP zostanie zablokowany, zanim wznowimy próbę ataku siłowego. Możemy również użyć opcji --fail - wait, aby ustawić czas, jaki reaver powinien odczekać po 10 nieudanych próbach. Możemy również użyć opcji -r, aby nakazać reaver uśpić na określoną liczbę sekund po określonej liczbie prób. Możemy skonfigurować opcję --timout, możemy eksperymentować z tymi opcjami, opcjami –delay i --fail - wait, jeśli punkt dostępowy blokował lub ignorował niektóre z naszych prób siłowych.

Teoria uzgadniania

W poprzedniej sekcji zobaczyliśmy, jak można wykorzystać funkcję WPS w routerach do złamania klucza WPA. Ten proces z pewnością zadziała w każdej sieci z włączonym WPS; dlatego jeśli Twój komputer docelowy używa szyfrowania WPA lub WPA2 i ma włączony WPS, powinna to być pierwsza metoda złamania hasła. Jeśli jednak WPS nie jest włączony, musimy złamać sam klucz WPA. Jak wyjaśniliśmy w sekcji poświęconej łamaniu zabezpieczeń WPS, w WPA każdy pakiet jest szyfrowany za pomocą unikalnego, tymczasowego klucza. Nie jest to tak jak w WEP, gdzie IV są powtarzane i zbieramy dużą liczbę pakietów danych z tymi samymi IV. W każdym pakiecie WPA znajduje się tymczasowy, unikalny IV. Nawet jeśli zbierzemy milion pakietów, nie będą one dla nas przydatne – nie zawierają żadnych informacji, które mogłyby pomóc nam ustalić rzeczywisty klucz WPA. Jedynymi pakietami zawierającymi informacje, które mogą pomóc nam ustalić klucz, są pakiety uzgadniania (handshake). Są to cztery pakiety wysyłane, gdy nowe urządzenie lub nowy klient łączy się z siecią docelową. Na przykład, gdy jesteśmy w domu i nasze urządzenie łączy się z siecią, mamy hasło, a między urządzeniem a punktem dostępowym zachodzi proces zwany czteroetapowym uzgadnianiem (ang. four-way handshake). W tym procesie cztery pakiety, zwane pakietami uzgadniania (ang. handshake), są przesyłane między dwoma urządzeniami w celu uwierzytelnienia połączenia urządzenia. Używając `aircrack-ng`, możemy użyć listy słów, testując każde hasło z listy za pomocą uzgadniania. Aby złamać szyfrowane sieci WPA, potrzebujemy dwóch rzeczy: przechwycenia uzgadniania i listy słów zawierającej hasła.

Przechwytywanie uścisku dłoni

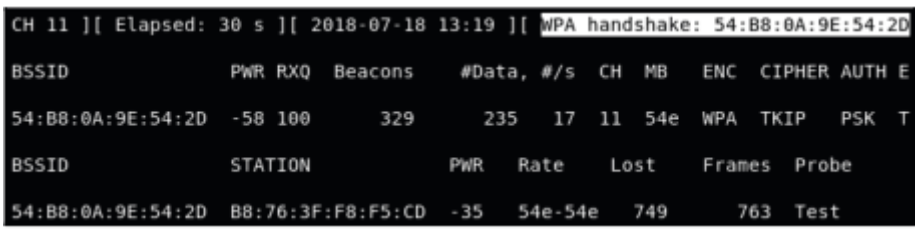
Aby złamać klucz WPA, pierwszą rzeczą, którą musimy zrobić, jest przechwycenie uścisku dłoni. Przechwycimy uścisk dłoni za pomocą `airodump-ng`, w ten sam sposób, w jaki używaliśmy go w sieciach szyfrowanych WEP. Użyjemy `airodump-ng --bssid`, w ten sam sposób, w jaki używaliśmy go w sieciach WEP; ostatecznie przechwytujemy tylko pakiety za pomocą `airodump-ng`, wykonuje on to samo zadanie. Dołączymy kanał, a następnie zapiszemy do pliku, wywołując plik `test-handshake`; dołączymy również kartę bezprzewodową w trybie monitorowania. Używamy tego samego polecenia, którego użyliśmy, przechwytując pakiety dla sieci WEP, `airodump-ng --bssid`. Umieszczamy docelowy AP, --channel; kanał docelowy, --write; nazwę pliku, w którym będziemy przechowywać dane; i wlan0, naszą kartę Wi-Fi, w trybie monitorowania. Polecenie wygląda następująco:

airodump-ng --bssid 54:B8:0A:9E:54:2D --channel 11 --write test-handshake wlan0

Po uruchomieniu tego polecenia będziemy mieli naszą sieć, sieć szyfrowaną WPA, z którą będzie połączony klient. Aby przechwycić uścisk dłoni, możemy po prostu usiąść i poczekać, aż urządzenie połączy się z siecią. Gdy urządzenie połączy się z siecią, możemy przechwycić uścisk dłoni lub skorzystać z czegoś, czego nauczyliśmy się w poprzednim rozdziale , czyli ataku deauthentication. W ataku deauthentication odłączamy od sieci każde urządzenie znajdujące się w zasięgu naszej sieci Wi-Fi. Jeśli zrobimy to na bardzo krótki okres czasu, możemy odłączyć urządzenie od sieci na sekundę; urządzenie spróbuje połączyć się z siecią automatycznie, a nawet osoba korzystająca z urządzenia nie zauważy, że jego urządzenie jest odłączane i ponownie podłączane. Będziemy wtedy mogli przechwycić pakiety uzgadniania. Ponownie powiedzieliśmy, że uzgadnianie jest wysyłane za każdym razem, gdy urządzenie łączy się z siecią docelową. Teraz po prostu uruchomimy podstawowy atak uwierzytelniania, używając `aireplay-ng`. Teraz umieścimy tylko małą liczbę: cztery pakiety deauthentication. Następnie wpisujemy -a, adres MAC docelowego punktu dostępowego, oraz -c, aby określić adres MAC klienta (adres MAC klienta, którego chcemy odłączyć). Następnie wpisujemy nazwę karty Wi-Fi, czyli wlan0 . Używamy `aireplay-ng --deauth`, nazwy ataku, oraz 4, pakietów uwierzytelniających do punktu dostępowego, po czym odłączamy od niego urządzenie. Polecenie wygląda następująco:

aireplay-ng --deauth 4 -a 54:B8:0A:9E:54:2D -c B8:76:3F:F8:F5:CD wlan0

Jak widać na poniższym zrzucie ekranu, przechwyciliśmy połączenie WPA, a nasze urządzenie docelowe w ogóle się nie zmieniło ani nie zostało odłączone:



Nie otrzymaliśmy żadnych komunikatów o rozłączeniu, ponieważ byliśmy rozłączeni przez bardzo krótki czas; w rezultacie nawet osoba korzystająca z urządzenia tego nie zauważyła, a my mogliśmy przechwycić uścisk dłoni. Teraz możemy użyć listy słów i porównać ją z uściskiem dłoni, aby spróbować ustalić główny klucz WPA.

Tworzenie listy słów

Po przechwyceniu uścisku dłoni wystarczy złamać klucz WPA, tworząc listę słów. Lista słów to po prostu lista słów, które `aircrack-ng` będzie sprawdzać, porównując każde z nich z uściskiem dłoni, aż do pomyślnego ustalenia klucza WPA. Im lepsza lista słów, tym większe szanse na złamanie klucza WPA. Jeśli hasło nie znajduje się w pliku z listą słów, nie będzie można ustalić klucza WPA. Użyjemy narzędzia o nazwie crunch. To w zasadzie po prostu skrypt; określamy znaki, które chcemy mieć w hasłach, a narzędzie tworzy wszystkie możliwe kombinacje tych haseł. Format polecenia do użycia crunch to crunch [min] [max]. [min] to minimalna liczba znaków hasła, które chcemy utworzyć, możemy powiedzieć, że chcemy minimum cztery, pięć, sześć itd. [max] to maksymalna liczba znaków w haśle. Możemy określić znaki, których chcemy używać w hasłach, na przykład abcdefg, wszystkie małe litery, a następnie możemy pisać wielkie litery; możemy wpisywać cyfry i symbole.

Opcja -t jest bardzo przydatna, jeśli znamy część hasła; jest to wzór. Na przykład, jeśli próbujemy odgadnąć hasło i widzieliśmy, jak ktoś je wpisuje, wiedząc, że zaczyna się od a i kończy na b, możemy użyć opcji wzoru i polecić crunch, aby tworzył hasła, które zawsze zaczynają się od a i kończą na b, a on umieści wszystkie możliwe kombinacje znaków, które wprowadziliśmy w poleceniu. Załóżmy, że chcemy utworzyć hasła składające się z co najmniej sześciu i maksymalnie ośmiu znaków, a hasła będą kombinacjami znaków 1, 2, 3, 4, 5 i 6 oraz symboli. Będzie on przechowywany w pliku o nazwie wordlist a wzór to wordlist. Hasła pliku zawsze będą zaczynać się od a i zawsze będą kończyć się b. Wszystkie hasła, które zobaczymy w pliku, będą zaczynać się od a i kończyć na b, i będą zawierać wszystkie możliwe kombinacje znaków, które określiliśmy między a a b. Uruchommy crunch i utwórzmy przykładową listę słów. Użyjemy crunch, a następnie ustawimy minimum 4 i maksimum 6. Po prostu wstawimy 123ab i zapiszemy go w `sample-wordlist`. crunch utworzy kombinację haseł (minimum cztery znaki, maksimum sześć znaków) i utworzy wszystkie możliwe kombinacje 123ab. Kombinacje zostaną zapisane w pliku o nazwie `sample-wordlist`. Polecenie będzie wyglądać następująco:

crunch 4 6 123ab -o sample-wordlist

Poniżej znajduje się wynik poprzedniego polecenia:

```
root@kali:~# crunch 4 6 123ab -o sample-wordlist
Crunch will now generate the following amount of data: 131250 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 19375

crunch: 100% completed generating output
```

Możemy odczytać hasło, uruchamiając polecenie `cat sample-wordlist`, i zobaczyć wszystkie hasła zapisane w pliku, jak pokazano na poniższym zrzucie ekranu:

```
root@kali:~# cat sample-wordlist
1111
1112
1113
111a
111b
1121
1122
1123
112a
112b
1131
1132
1133
113a
113b
11a1
11a2
11a3
11aa
11ab
11b1
11b2
11b3
```

Możemy zobaczyć wszystkie hasła utworzone przez crunch. Im dłuższe hasło i im więcej znaków w nim umieścimy, tym więcej haseł możemy utworzyć i tym więcej miejsca zajmą. Przyjrzyjmy się opcji wzorca. Przejdziemy do crunch, używając minimum 5 i maksimum 5, więc wszystkie hasła będą miały pięć znaków, a następnie wprowadzimy znaki, które są 123ab (jak poprzednio), i dodamy opcję -t, która jest opcją wzorca. Następnie powiemy, że hasło zaczyna się od a i kończy na b, i chcemy uzyskać wszystkie możliwe kombinacje znaków między a i b. Następnie określimy plik wyjściowy -o; nazwijmy go `pattern-wordlist`. Oto polecenie:

crunch 5 5 123ab -t a@@@b -o pattern-wordlist

Wynik będzie następujący:

```
root@kali:~# crunch 5 5 123ab -t a@@@b -o pattern-wordlist
Crunch will now generate the following amount of data: 750 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 125

crunch: 100% completed generating output
```

Tworzy 125 haseł; przyjrzyjmy się im. Jak widać na poniższym zrzucie ekranu, zawsze zaczynają się od a i zawsze kończą na b:

```
root@kali:~# cat pattern-wordlist
a111b
a112b
a113b
a11ab
a11bb
a121b
a122b
a123b
a12ab
a12bb
a131b
a132b
a133b
a13ab
a13bb
a1a1b
a1a2b
a1a3b
a1aab
a1abb
a1b1b
a1b2b
```

Możemy użyć programu crunch do utworzenia listy słów, a w następnej sekcji wykorzystamy listę słów i plik uzgadniania, aby ustalić rzeczywisty klucz WPA.

Łamanie listy słów

Teraz, gdy przechwyciliśmy uścisk dłoni z naszego docelowego punktu dostępowego i mamy gotową do użycia listę słów, możemy użyć `aircrack-ng`, aby złamać klucz dla docelowego punktu dostępowego. `aircrack-ng` przeszuka plik listy słów, połączy każde hasło z nazwą naszego docelowego punktu dostępowego i utworzy klucz główny parowania (PMK). Klucz główny parowania jest tworzony za pomocą algorytmu o nazwie PBKDF2. Nie polega on tylko na połączeniu hasła i identyfikatora BSSID; jest on szyfrowany w określony sposób i porównywany z uściskiem dłoni. Jeśli klucz główny parowania był prawidłowy, użyte hasło jest hasłem dla docelowego punktu dostępowego. Jeśli nie było prawidłowe, `aircrack-ng` próbuje kolejnego hasła. Używamy `aircrack-ng`, nazwy pliku zawierającego uzgadnianie, test-handshake-01.cap, oraz `-w` i nazwy listy słów, wordlist. Polecenie wygląda następująco:

aircrack-ng test-handshake-01.cap -w wordlist

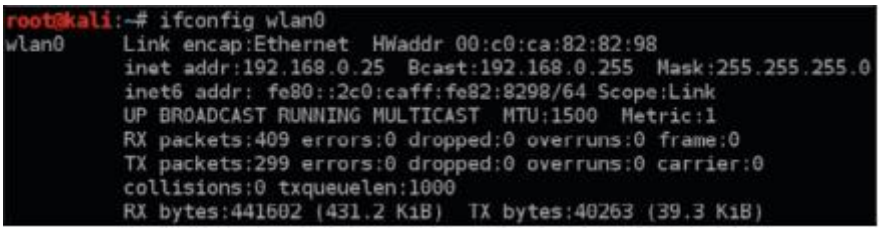
Teraz naciskamy Enter, a polecenie `aircrack-ng` przeszuka listę; wypróbuje wszystkie hasła i połączy każde z nazwą docelowego punktu dostępowego (AP), aby utworzyć klucz PMK, a następnie porówna go z uzgadnianiem. Jeśli klucz PMK jest prawidłowy, hasło użyte do utworzenia klucza PMK jest hasłem docelowego punktu dostępowego; jeśli klucz PMK nie jest prawidłowy, spróbuje po prostu użyć kolejnego hasła. Jak widać na poniższym zrzucie ekranu, klucz został znaleziony:

```
                      Aircrack-ng 1.2

[00:00:08] 2576/15624 keys tested (307.39 k/s)

Time left: 42 seconds                                 16.49%

                     KEY FOUND! [ a1b1a11b ]


Master Key     : 75 90 9C FB 3B 3B 71 56 4B 6E C5 A8 97 EC 19 15
                 5F BF FF C3 27 67 16 D8 68 69 D1 94 F2 83 8F 69

Transient Key  : 5C 50 8C 7A 97 CD 4B 1A 69 42 34 63 25 3C BD 2E
                 D2 D2 FF 26 3F A5 D2 7A B9 A3 FB 77 3A 4F 86 D2
                 3B D9 23 7E C9 A9 1D AF AE 0D C0 5F 95 DC D4 82
                 B7 EB BD 5C AE 11 19 41 40 C4 B9 A7 62 88 F1 0C

EAPOL HMAC     : 25 7D AC 00 9D 6D 9D AC 05 4D 6A 1E D0 FD 41 99
```

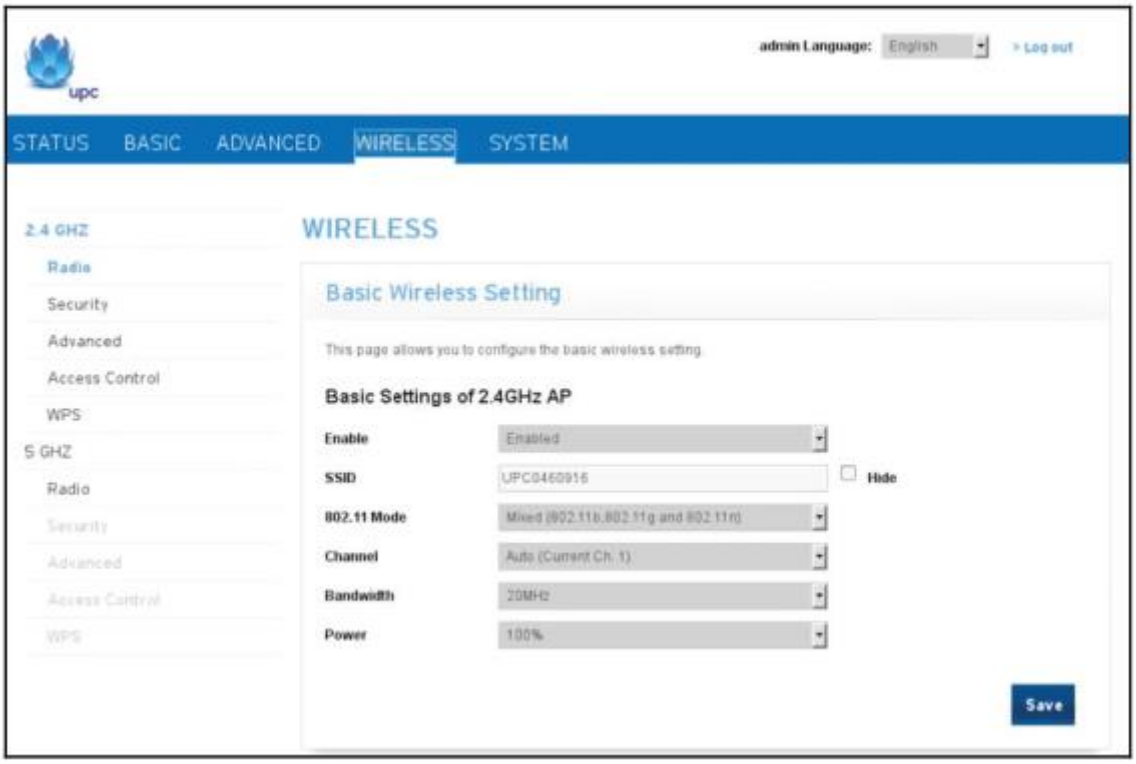
To najprostszy sposób użycia listy słów: złamanie hasła zajęło 42 seconds. Szybkość zależy od szybkości procesora i od tego, czy uruchomione są jakieś procesy, które spowalniają działanie komputera.

Zabezpieczanie sieci przed atakami

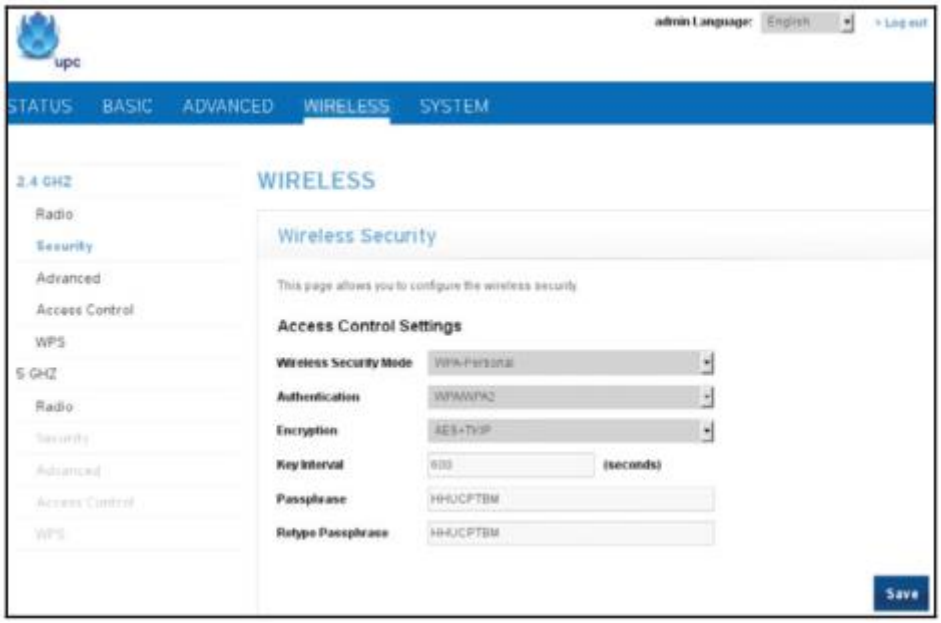
Aby zapobiec włamaniom do sieci za pomocą metod opisanych w rozdziale, musimy uzyskać dostęp do strony ustawień routera. Każdy router ma stronę internetową, na której użytkownik może modyfikować ustawienia routera, zazwyczaj pod adresem IP routera. Najpierw pobieramy adres IP mojego komputera lub urządzenia i uruchamiamy polecenie ifconfig wlan0; jak widać na poniższym zrzucie ekranu, wyróżniona część to adres IP komputera:



Teraz otwórz przeglądarkę i przejdź do 192.168.0.1; w tym przykładzie adres IP komputera to 25. Zwykle adres IP routera jest pierwszym adresem IP podsieci. W tej chwili jest to 192.168.0.0, a my po prostu dodamy cyfrę 1, ponieważ jest to pierwszy adres IP w podsieci, co przeniesie nas do strony ustawień routera. Na stronie ustawień zostaniesz poproszony o podanie nazwy użytkownika i hasła. Routery są dostarczane z predefiniowaną nazwą użytkownika i hasłem — możemy sprawdzić, jakie są domyślne nazwy użytkownika i hasła; zdecydowanie zaleca się ich późniejszą zmianę. Zazwyczaj jest to opisane w instrukcji, więc sprawdź instrukcję, sprawdź domyślną nazwę użytkownika i hasło, a następnie zaloguj się, używając tych danych. W niektórych przypadkach atakujący może przeprowadzać atak deauthentication, uniemożliwiając nam bezprzewodowe połączenie z siecią. Możemy połączyć się z routerem za pomocą kabla Ethernet; gdy to zrobimy, atakujący nie będzie mógł użyć ataku deauthentication, aby nas deauthentication lub rozłączyć, a my będziemy mogli uzyskać dostęp do ustawień routera za pomocą kabla. Możemy zmodyfikować nasze ustawienia zabezpieczeń i zmienić szyfrowanie, zmienić hasło i wykonać wszystkie zalecane czynności w celu zwiększenia bezpieczeństwa, aby atakujący nie mógł zaatakować sieci i uzyskać klucza.Ustawienia każdego routera są różne; zależą od producenta, a nawet modelu routera. Zazwyczaj jednak sposób zmiany ustawień jest taki sam; w 90% przypadków router zawsze znajduje się na pierwszym adresie IP podsieci, wystarczy pobrać adres IP za pomocą polecenia ifconfig, tak jak zrobiliśmy to na początku tego tematu. Otrzymaliśmy adres IP 192.168.0.25, a następnie zmieniliśmy ostatnie 25 na liczbę 1 pierwszego adresu IP, co stanowi adres IP naszego routera. Teraz przejdziemy do ustawień WIRELESS. Jak widać, istnieje wiele ustawień, które możemy zmienić dla naszej sieci, a na razie interesują nas ustawienia WIRELESS:

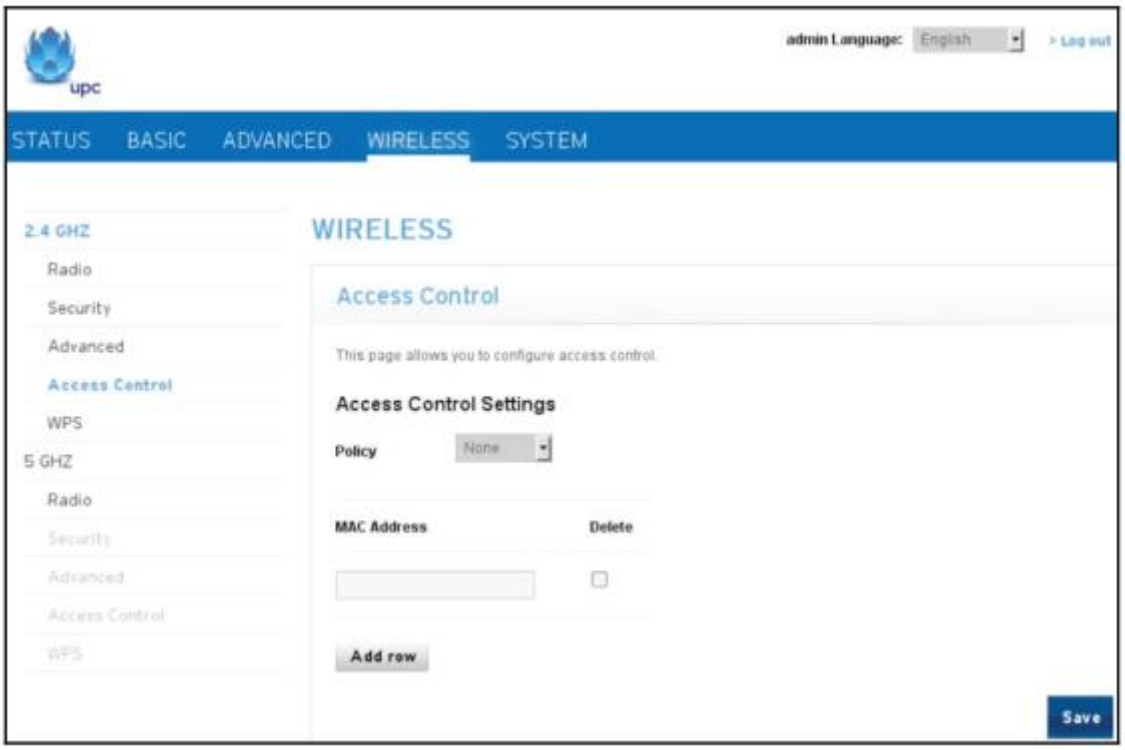


Jak widać na poprzednim zrzucie ekranu, ustawienia sieci bezprzewodowej są włączone, możemy nawet zmienić nazwę sieci w polu SSID; możemy również zmienić kanał i przepustowość. Po przejściu do opcji Bezpieczeństwo, jak widać na poniższym zrzucie ekranu, używamy szyfrowania WPA z uwierzytelnianiem WPA/WPA2, a szyfrowanie wykorzystuje AES+TKIP:



Jeśli przejdziemy do WPS, możemy zobaczyć, że WPS jest wyłączony; nie używamy WEP, więc atakujący nie mogą wykorzystać żadnego z ataków w celu złamania szyfrowania WEP:

Używamy WPA, które jest znacznie bezpieczniejsze, i wyłączyliśmy WPS, aby ataki nie mogły użyć reaver do ustalenia kodu PIN WPS, a następnie zinterpretować hasła metodą inżynierii wstecznej. Jedynym sposobem, w jaki haker może uzyskać dostęp do hasła lub je zdobyć, jest najpierw uzyskanie potwierdzenia, a następnie użycie listy słów do znalezienia hasła. Hasło jest bardzo losowe, mimo że nie zawiera cyfr ani cyfr, a jedynie litery; jest jednak bardzo losowe, więc istnieje bardzo małe prawdopodobieństwo, że ktoś je odgadnie. Teraz mamy również kontrolę dostępu; dzięki niej możemy dodać polityki, takie jak polityka zezwalania lub odmowy:



Możemy określić adresy MAC, którym chcemy zezwolić na połączenie z naszą siecią; możemy również określić adresy MAC, którym chcemy zabronić dostępu do naszej sieci. Na przykład, jeśli w Twoim domu nie ma wielu osób ani gości, albo jeśli pracujesz w firmie z określoną liczbą komputerów i chcesz zezwolić na połączenie z siecią tylko określonej liczbie komputerów, możesz uzyskać ich adresy MAC (dla osób, którym chcesz zezwolić) i dodać je do listy dozwolonych. Nawet jeśli ktoś ma rzeczywisty klucz i nie znajduje się na białej liście ani na liście dozwolonych, nie będzie mógł uzyskać dostępu do sieci. Możemy również dodać listę odrzuconych, gdy chcemy odmówić dostępu określonemu

komputerowi lub osobie, którą uważamy za podejrzaną; wystarczy, że dodamy ich adres MAC do listy odrzuconych, a oni nie będą mogli połączyć się z Twoją siecią:

Strona ustawień routera zazwyczaj wygląda inaczej dla różnych routerów; nazwy opcji mogą się różnić, ale najważniejsze jest to, żebyśmy mogli uzyskać dostęp do ustawień routera, używając adresu IP podsieci i dodając na końcu cyfrę 1, która jest pierwszym adresem IP. Jeśli jesteś atakowany i w ogóle nie możesz połączyć się z siecią, po prostu użyj kabla i zmodyfikuj ustawienia, tak jak omówiliśmy.

Podsumowanie

W tym rozdziale omówiliśmy, jak łatwo jest złamać sieci szyfrowane WEP, nawet jeśli do sieci docelowej nie są podłączone żadne urządzenia i sieć jest bezczynna. Poznaliśmy również szereg metod wstrzykiwania pakietów do ruchu i powodowania bardzo szybkiego wzrostu ilości danych, aby złamać klucz WEP w bardzo krótkim czasie. Następnie przeanalizowaliśmy wszystkie słabości, które hakerzy mogą wykorzystać do włamania się do sieci szyfrowanych WEP, WPA i WPA2. Następnie zobaczyliśmy, jak hakerzy mogą wykorzystać te słabości do łamania haseł i zdobywania kluczy do sieci. Później, jako atakujący, będziemy mogli dezaktywować lub odłączyć dowolne urządzenie od dowolnej sieci bez konieczności znajomości klucza. Pod koniec rozdziału omówiliśmy, jak możemy modyfikować ustawienia naszych routerów, aby zwiększyć szyfrowanie i bezpieczeństwo sieci, uniemożliwiając hakerom przeprowadzanie ataków i zdobywanie haseł. W następnym rozdziale dowiemy się, jak gromadzić informacje, a także jak korzystać z różnych narzędzi, które pozwolą nam uzyskać bardziej szczegółowe informacje za pomocą różnych skanów i generowanych raportów.