HACK EENS... EEN DRAADLOOS NETWERK

Iedereen roept enthousiast hoe eenvoudig draadloze netwerken te hacken zijn, maar slechts weinigen laten vervolgens ook zien dat het werkelijk zo eenvoudig is. Dat is jammer, want met een paar eenvoudige handelingen - op uw eigen netwerk, welteverstaan - komt u te weten hoe makkelijk uw netwerk werkelijk te hacken is. Daarna kunt u maatregelen nemen om de beveiliging aan te scherpen en die vervolgens wederom testen.

Om goed te kunnen testen, heeft u de volgende hardware nodig: een USB-stick met minstens 1 GB opslagcapaciteit en twee computers die draadloos met het internet kunnen verbinden. Eén van deze machines gaan we gebruiken voor het hackwerk en de andere gaat dienstdoen als gesimuleerd slachtoffer. Hou er rekening mee dat u met deze test gereedschap heeft om bij de buren binnen te komen, maar dat dit bepaald niet beleefd is; het is niet de bedoeling dat u inbreekt en de juridische gevolgen van dergelijke onbeleefdheid zijn voor uw eigen rekening.

Opstartbare USB-stick

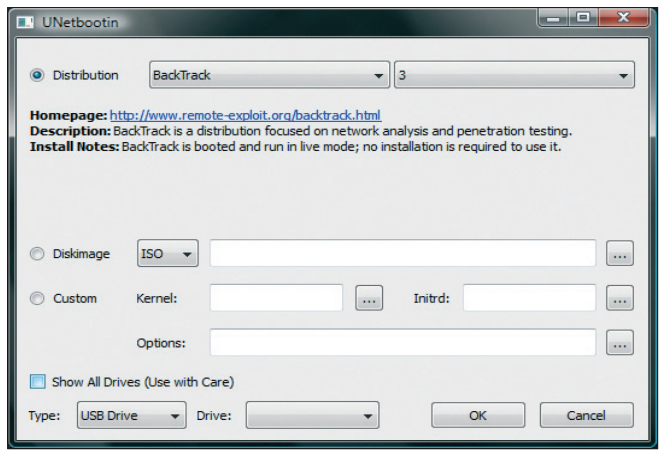
Als u de hardware bij elkaar heeft, dient u UNetBootin van het internet (http://unetbootin.sourceforge.net/) of onze cover-cd te halen. Dit is een zeer plezierige applicatie om opstartbare USB-sticks met Linux mee te maken. Steek uw USB-stick in de computer en start daarna de applicatie (u hoeft niets te installeren). Geef onderin het venster aan dat u een USB-drive wilt gebruiken en geef in het uitrolmenu de juiste driveletter aan. Aan de bovenkant van het venster kunt u kiezen uit een reeks Linux-distributies. Selecteer hier de Backtrack-distributie en geef bij versie NUMMER 3 aan. Druk vervolgens op OK en wacht rustig af tot uw USB-stick geformatteerd en geïnstalleerd is. UNetBootin downloadt zelf alle benodigde bestanden voor uw distributie, dus u hoeft weinig werk te verzetten. Het lijkt wel alsof de applicatie vastloopt; door geduldig te wachten en niet op de knoppen te drukken, moet u binnen ongeveer een uur (mede afhankelijk van uw internetverbinding) de installatie rond hebben.

Na de installatie verwijdert u de USB-stick uit uw systeem en negeert u de boodschap dat u moet herstarten; die is alleen relevant als u van plan bent om direct met dat systeem via USB te starten. Vervolgens plaatst u deze stick, die we voor het gemak 'blikopener' noemen, in het systeem waarmee u de aanval op uw netwerk in wilt zetten. Als er keuze is, gebruik dan voor dit systeem de krachtigste draadloze netwerkcomputer die u heeft. Start vervolgens met de USB-drive en wacht tot de Linux-omgeving geladen is.

Verkennen

De eerste stap naar een draadloze hack is verkennen. Natuurlijk is dat niet nodig aangezien u al bekend bent met uw systeem, maar omdat we doen alsof we van niets weten, gaan we toch door de stappen heen. De meest overzichtelijke applicatie om mee op verkenning te gaan is Kismet. Start dit door naar de K linksonder in beeld te gaan (het equivalent van de Start-knop in Windows). Kies vervolgens BACKTRACK | RADIO NETWORK ANALYSIS | 80211 | ANALYSER | KISMET. Nog makkelijker is klikken op de monitor naast de K; er verschijnt dan een commandoprompt waar u simpelweg KISMET typt.

Het Kismet-venster laat alle gedetecteerde draadloze netwerken in de omgeving zien. Als het netwerk op standje 'verborgen' staat, krijgen we hier te zien hoeveel karakters de naam lang is. Het kost dan iets meer moeite om dit netwerk te kraken. Voor ons is de term onder kolom W het belangrijkst. Staat hier een N, dan is het een onbeveiligd netwerk. Daar hebben we niets aan, want daar kan ieder-



Met UNetBootin is het maken van een opstartbare USB-stick een fluitje van een cent.

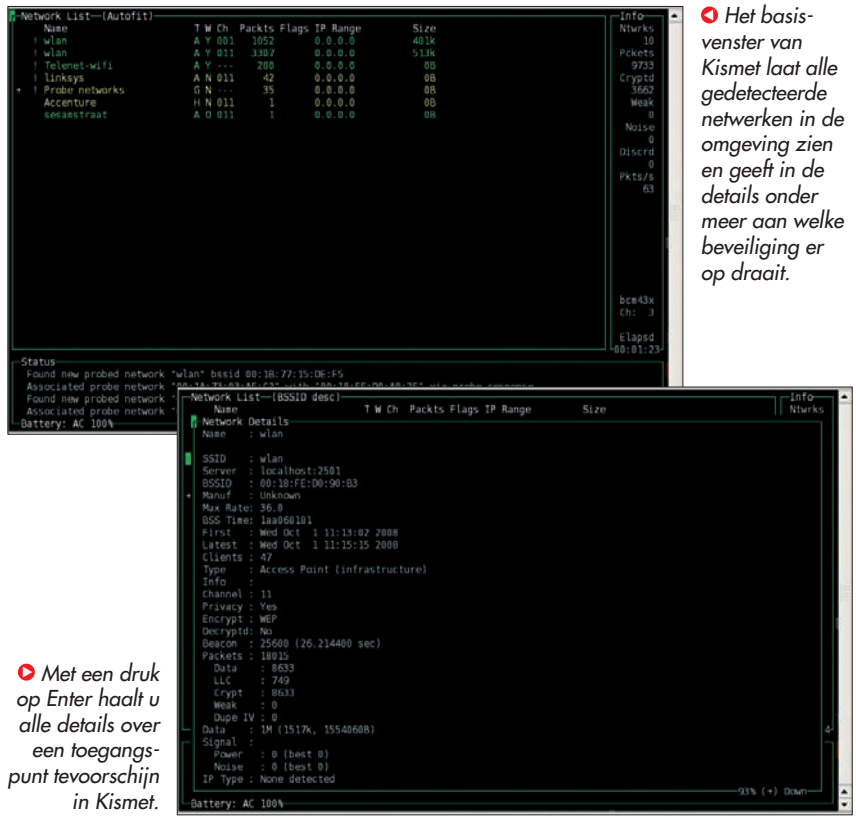
een binnen. Staat er een Y, dan heeft het netwerk WEP-encryptie; staat er een O, dan heeft het netwerk WPA-beveiliging in een variant.

WEP kraken

We zetten bij onze eerste gesimuleerde aanval de draadloze router op WEP-encryptie en geven een sleutel in. In Kismet zien we dan een Y in kolom W staan. We doen alsof we verder niets over het netwerk weten en gaan daarom eerst de belangrijkste details achterhalen. Druk in Kismet eerst op de S en dan nogmaals op de S om de netwerken te rangschikken op naam. We kunnen dan met de cursortoetsen naar ons testnetwerk en drukken daar op ENTER. We krijgen een lijst met alle details over het netwerk in kwestie. Voor ons zijn drie zaken van belang: SSID, BSSID en Channel. SSID is de naam van het netwerk, BSSID het MAC-adres van de router en Channel het kanaal waarin wordt uitgezonden.

Schrijf die details op een papiertje of laat het venster met Kismet in de hoek van het beeld openstaan. Open nu een tweede commandoprompt. Typ hier het volgende commando: AIRODUMP-NG -W KRAAK --IVS --BSSID <MAC ADRES ROUTER> -A --CHANNEL <NR> ETH0. De toevoeging -w kraak geeft aan dat de bestanden die we nu gaan afvangen allemaal beginnen met de naam 'kraak'. Met –ivs geven we aan dat alleen afgevangen pakketten opgeslagen moeten worden en niet alles wat de kaart oppikt. Bij –bssid vullen we het MAC-adres van de router in (dat we in Kismet gevonden hebben). De aanduiding -a geeft aan dat we sleutels van computers die niet met een toegangspunt verbonden zijn niet willen opslaan (dat spaart ruimte in ons geheugen en daar hebben we toch niets aan). Bij –channel geven we het nummer van het kanaal in (zie wederom Kismet) en om af te sluiten, moet u in plaats van eth0 de naam van uw netwerkinterface aangeven. Dit kunt u achterhalen door in de commandoprompt eerst IFCONFIG -A te typen; er verschijnt dan een lijstje van uw netwerkverbindingen met hun Linux-naam.

Na het ingeven van dit commando verschijnt in de commandoprompt een overzicht waarop u bovenin details over het toegangspunt ziet en onderin kunt zien wie er met het toegangspunt verbonden is (gebaseerd op het MAC-adres). Belangrijk in de onderste rij is de term PACKETS. Hoe hoger het getal hier, hoe groter de kans dat u de sleutel kunt kraken.



Het basisvenster van Kismet laat alle gedetecteerde netwerken in de omgeving zien en geeft in de details onder meer aan welke beveiliging er op draait.

Met een druk op Enter haalt u alle details over een toegangspunt tevoorschijn in Kismet.

Het goede nieuws is dat u tijdens het afvangen van pakketten al een aanval op de sleutel kunt doen. Open daarvoor een derde commandovenster en typ hier AIRCRACK-NG -E <SSID> KRAAK*.IVS. Bij de -e geeft u de naam van het netwerk in (SSID). Aircrack gaat vervolgens aan het rekenen met de pakketten die binnen zijn. Hoe meer pakketten er zijn, hoe sneller de berekening gaat. Op onze testopzet werd het wachtwoord gekraakt na het afvangen van iets meer dan 200.000 pakketten; het afvangen van de pakketten nam 6 minuten in beslag, het doorrekenen van het wachtwoord 5 seconden.

Nu is het probleem bij een testnetwerk dat er maar heel weinig verkeer wordt gegenereerd. We kunnen dit versnellen door verkeer tussen de router en het toegangspunt na te bootsen. Om dit te doen, opent u een vierde commandoprompt en typt u AIREPLAY-NG --ARPREPLAY -B <MAC ADRES ROUTER> -H <MAC ADRES VAN DE VERBONDEN COMPUTER> ETH0. Het MAC-adres van de verbonden computer kunt u terugvinden in het commandovenster waar u AIRODUMP-NG uitvoert. Dat staat in de onderste rij vermeld. Als alternatief kunt u in Kismet op het toegangspunt gaan staan en dan op de C drukken; er verschijnt dan een lijst van MAC-adressen van verbonden computers.

WPA kraken

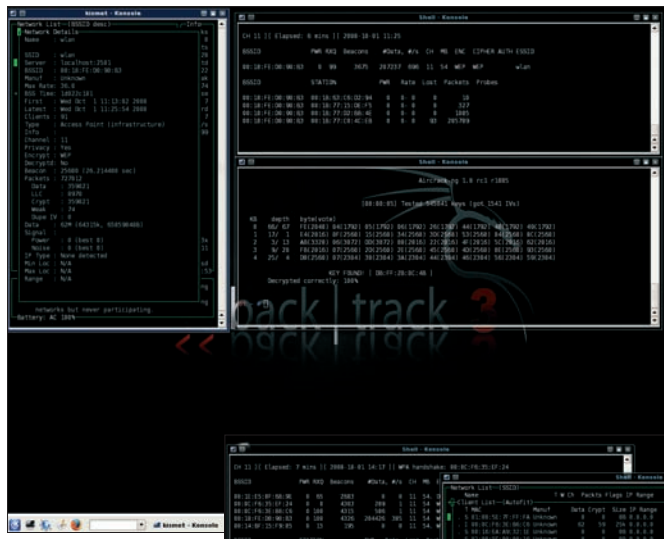
Gelukkig wordt WEP tegenwoordig bijna niet meer toegepast. Standaard is tegenwoordig een vorm van WPA-beveiliging. Dat bestaat globaal gezien in twee smaken: met TKIP of met RADIUS-beveiliging. Bij RADIUS-beveiliging wordt het verbinden via een aparte server afgehandeld; we zien dit daarom eigenlijk alleen in bedrijven. RADIUS is te kraken in de zin dat alles te kraken is, maar eenvoudig is het niet. We kunnen daarom veilig stellen dat we als normale gebruiker daar niet bij kunnen.

Op normale routers voor thuisgebruik wordt gebruikgemaakt van TKIP. Daar zit een probleem aan dat bij het aanmelden van een computer op het netwerk het wachtwoord versleuteld wordt verstuurd naar de router en de router daarna een goedkeuring met sleutel terugstuurt. Dit is in de statistieken die we afvangen terug te vinden. De truc met WPA-wachtwoorden is daarom wachten tot er iemand op het netwerk inlogt.

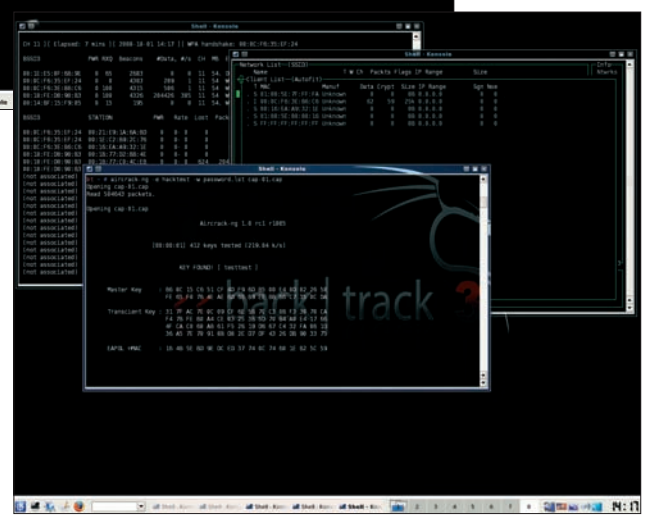
→

We gebruiken voor onze testopstelling wederom het airodump-commando. Vervolgens loggen we met de tweede draadloze computer in op het draadloze netwerk. Als Airodump erin slaagt de sleutel te onderscheppen, verschijnt er rechtsboven in het venster de term WPA-handshake. We hebben dan de sleutel op de computer staan.

Om deze sleutel te kraken, maken we wederom gebruik van aircrack-ng; dit keer in combinatie met een woordenlijst. Door te zoeken met Google kunt u een keur aan woordenlijsten ophalen, bijvoorbeeld die op www.openwall.com/passwords/wordlists. Hier kunt u betalen voor complete woordenlijsten in meerdere talen of onderaan de pagina een gratis bestand met 3.000 standaardwachtwoorden ophalen (password.lst). Zet dit bestand op een USB-stick en kopieer het naar de Home-map van uw draaiende Backtrack-besturingssysteem.



Ons met WEP beveiligde testnetwerk, WLAN, wisten we in 6 minuten en 5 seconden te kraken.



Het kraken van ons netwerk dat met WPA in combinatie met een te licht wachtwoord was beveiligd nam 7 minuten en 1 seconde in beslag; 7 minuten om onze testmachine in te loggen en 1 seconde om het wachtwoord te kraken.

Wachtwoord kraken

Vervolgens geeft u als commando AIRCRACK-NG –E <SSID NAAM> -W PASSWORD.LST KRAAK-01.CAP. Daarbij vult u bij 'SSID naam' de naam van uw router in. Als u een andere wachtwoordlijst heeft opgehaald, geeft u die naam in bij PASSWORD.LST; werkt u met een andere bestandsnaam dan 'kraak' of heeft u meerdere keren Airodump gestart, dan dient u de bestandsnaam van kraak-01.cap te veranderen naar de naam en het pogingnummer waarin u de aanval heeft uitgevoerd. Aircrack gaat vervolgens met de wachtwoordenlijst rekenen en voert daar een paar standaardtrucs van gebruikers op uit. Zo werd binnen één seconde ons wachtwoord 'testtest' uit de bestanden gefilterd.

Heeft u wat nummers toegevoegd aan een standaardwoord uit het woordenboek, dan moet u waarschijnlijk een net iets complexere kraakpoging uitvoeren door de kraaktool van John The Ripper aan te spreken. Dat doet u door het volgende commando uit te voeren: 'JOHN --WORDLIST=PASSWORD.LST –RULES –STDOUT | AIRCRACK-NG –E SSID –W - KRAAK-01.CAP'. U geeft hiermee opdracht om de applicatie John met de password.lst-woordenlijst te laten werken met standaardregels en de uitvoer van dit commando in te voeren in uw aircrack-ng-commando. Als u dan nog geen resultaat haalt, kunt u meer kraakinformatie vinden op www.openwall.com/john.

Veilig netwerken

Door ons eigen netwerk te hacken kunnen we de beveiliging flink verbeteren. Les één mag heel duidelijk zijn: gebruik geen WEP-encryptie. Het netwerk is dan gegarandeerd binnen tien minuten met standaardtools open te breken. WPA is een stuk beter. Werken met RADIUS is voor normale huishoudens en kleine bedrijven geen praktische oplossing; gelukkig is TKIP op zich veilig genoeg als u een paar regels in acht neemt.

Gebruik om te beginnen geen standaardwoorden uit het woordenboek om uw netwerk af te schermen, zelfs niet een paar woorden die aan elkaar geplakt zijn. Onze testmachine is niet de snelste op de planeet en die loopt alle mogelijke combinaties in het woordenboek met 219 per seconde na. Probeer ook niet uw netwerk af te schermen door een paar letters door cijfers te veranderen; dat vertraagt onze rekenoperatie maar een klein beetje. Wilt u redelijk veilig zijn, gebruik dan een sterk wachtwoord van een stuk of twaalf willekeurige karakters. Gebruik bijvoorbeeld www.pctools.com/guides/password/ om een sterk wachtwoord te genereren. Hang dit wachtwoord desnoods thuis ergens op of gebruik de mogelijkheid van Vista om computers die u op het netwerk wilt toelaten met een USB-stick automatisch van dit wachtwoord te voorzien.

Om af te sluiten nog twee laatste tips. Als eerste: de optie om uw netwerk te verbergen door het SSID te verbergen helpt niet; de tools die we gebruiken kunnen dat eenvoudig kraken. Het maakt het instellen van uw draadloze netwerk daarom alleen maar lastiger. En als tweede: vertrouw niet op MAC-filtering om uw netwerk te beveiligen. Een aanvaller kan zien welke MAC-adressen contact mogen maken en kan eenvoudig dit adres nabootsen voor de aanvalsmachine, terwijl u voor normale gastgebruikers veel extra moeite moet doen om de router correct open te stellen. [M.G.]