



مرکز تخصصی آیا دانشگاه کردستان

انواع حملات شبکه های Wi-Fi و ابزارهای ارزیابی امنیتی آن (قسمت اول)

نویسنده

مسلم حقیقیان

شماره سند: A96001

۱۳۹۷/۰۰/۰۰



www.cert.uok.ac.ir



apa@uok.ac.ir



087-33662932



مقدمه

باوجود آنکه به نظر می‌رسد که از نظر فنی عبارت شبکه بی‌سیم جهت اشاره به هر نوع «شبکه‌ای» که «بی‌سیم» باشد بکار می‌رود، این اصطلاح بیشتر برای اشاره به «شبکه‌های ارتباطی» بکار می‌رود که در آن «گره‌ها» بدون استفاده از سیم به یکدیگر متصل می‌شوند، برای نمونه یک «شبکه رایانه‌ای» که نوعی از شبکه‌های ارتباطی است. از آنجاکه شبکه‌های بی‌سیم، در دنیای کنونی هرچه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه‌ها، که بر اساس سیگنال‌های رادیویی‌اند، مهم‌ترین نکته در راه استفاده از این فناوری، آگاهی از نقاط قوت و ضعف آن است. نظر به لزوم آگاهی از خطرات استفاده از این شبکه‌ها، باوجود امکانات نهفته در آن‌ها که به مدد پیکربندی صحیح می‌توان به سطح قابل قبولی از بعد امنیتی دست‌یافت، بنا داریم در این مقاله به بررسی حملات در شبکه‌های بی‌سیم و معرفی ابزارهای موردنیاز در آزمون نفوذپذیری آن بپردازیم.

کلمات کلیدی

ارزیابی امنیتی 802.11، WEP, WPA1, WPA2, TKIP, Krack, eifi pentest tools، سرقت پاکت‌های وایرلس، WPS، تزریق در شبکه وایرلس، sniff

رفع مسئولیت:

این مقاله صرفاً جنبه‌ی آموزشی دارد و به منظور ارتقا سطح علمی مسئولین آیتی و مسئولین امنیتی و جهت استفاده در تحقیقات دانشگاهی نوشته شده است. هرگونه بهره‌برداری غیراخلاقی و یا مخرب از آن صرفاً به عهده‌ی خود شخص است و نویسنده‌ی مقاله هیچ‌گونه مسئولیتی را در قبال استفاده‌ی نادرست از آن را نمی‌پذیرد.

فهرست مطالب

استاندارد ۸۰۲,۱۱	۱-
کانال‌های ۸۰۲,۱۱	۲-
انواع حالت‌های Wifi	۳-
حالت Master	۳-۱-
حالت Managed	۳-۲-
حالت Ad-hoc	۳-۳-
حالت Monitoring	۳-۴-
Mesh network/cloud	۳-۵-
Repeaters	۳-۶-
نام شبکه‌های وایرلس	۴-
SSID	۴-۱-
BSSID - چیست ؟	۴-۲-
ESSID - چیست ؟	۴-۳-
آنتن مناسب در آزمون نفوذ وایرلس	۵-
آنتن جهت‌دار (Directional)	۵-۱-
آنتن چندجهته (Omni-Directional)	۵-۲-
آنتن شبکه‌ی سهمی‌وار	۳-۵-
آنتن Yagi	۴-۵-
آنتن دوقطبی	۵-۵-
چیپست مناسب	۶-
فریم‌های شبکه ۸۰۲,۱۱	۷-
فریم کنترل Frame Control	۷-۱-
فریم‌های مدیریتی - پیوستن به شبکه و ترک آن (Management Frames)	۷-۲-
درخواست پیوستن به شبکه (Association request)	۷-۲-۱-
ترک شبکه (Disassociation)	۷-۲-۲-
فریم‌های مدیریتی - پیوستن مجدد به شبکه (Reassociation)	۷-۲-۳-
احراز هویت: (Authentication)	۷-۲-۴-
لغو حضور و سلب هویت (Deauthentication)	۷-۲-۵-
تبادل امن (Secure Communication)	۷-۲-۶-
احراز هویت:	۷-۳-
دعوت از ایستگاه‌ها با فریم (Beaconing)	۷-۴-
گزارش در خصوص فریم‌های آماده ارسال (ATIM)	۷-۵-
مکانیزم رومینگ یا Handover	۷-۶-
رمزنگاری در شبکه‌های بی‌سیم و ضعف‌های امنیتی آن‌ها	۸-
رمزنگاری WEP چیست ؟	۸-۱-
ضعف‌های امنیتی WEP	۸-۲-
WPA یا Wi-Fi Protected Access	۸-۳-

- ۸-۴- WPA چگونه کار می کند ؟
- ۵-۸- WPA2 - چیست ؟
- ۸-۶- WPA2 چگونه عمل می کند ؟
- ۸-۷- مشکلات امنیتی WPA/WPA2
- ۹- امنیت
- ۹-۱- محرمانگی (Confidentiality)
- ۹-۲- یکپارچگی (Integrity)
- ۹-۳- دسترس پذیری (Availability)
- ۹-۴- انواع حملات شبکه های وایرلس
- ۹-۵- حملات کنترل دسترسی
- ۹-۶- حملات علیه محرمانگی
- ۹-۷- حملات یکپارچگی
- ۹-۸- حملات علیه احراز هویت
- ۹-۹- حملات علیه در دسترس بودن
- ۱۰- معرفی ابزار

۱- استاندارد 802.11

انجمن IEEE در ماه ژوئن سال ۱۹۹۷ استاندارد IEEE 802.11-1997 را به‌عنوان اولین استاندارد شبکه‌های محلی بی‌سیم منتشر کرد. این استاندارد در سال ۱۹۹۹ مجدداً بازنگری شد و نسخه به‌روز شده آن تحت عنوان IEEE 802.11-1999 منتشر شد. استاندارد جاری شبکه‌های محلی بی‌سیم یا همان IEEE 802.11 تحت عنوان ISO/IEC 8802-11:1999، توسط سازمان استانداردسازی بین‌المللی (ISO) و مؤسسه استانداردهای ملی آمریکا (ANSI) پذیرفته شده است. تکمیل این استاندارد در سال ۱۹۹۷، شکل‌گیری و پیدایش شبکه‌سازی محلی بی‌سیم و مبتنی بر استاندارد را به دنبال داشت. استاندارد ۱۹۹۷، پهنای باند ۲Mbps را تعریف می‌کند با این ویژگی که در شرایط نامساعد و محیط‌های دارای اغتشاش (نویز) این پهنای باند می‌تواند به مقدار ۱Mbps کاهش یابد. روش تلفیق یا مدولاسیون در این پهنای باند روش DSSS است. بر اساس این استاندارد پهنای باند ۱Mbps با استفاده از روش مدولاسیون FHSS نیز قابل‌دستیابی است و در محیط‌های عاری از اغتشاش (نویز) پهنای باند ۲Mbps نیز قابل‌استفاده است. هر دو روش مدولاسیون در محدوده باند رادیویی ۲,۴GHz عمل می‌کنند. یکی از نکات جالب‌توجه در خصوص این استاندارد استفاده از رسانه مادون‌قرمز علاوه بر مدولاسیون‌های رادیویی DSSS و FHSS به‌عنوان رسانه انتقال است. ولی کاربرد این رسانه با توجه به محدودیت حوزه عملیاتی آن نسبتاً محدود و نادر است. گروه کاری ۸۰۲,۱۱ به زیرگروه‌های متعددی تقسیم می‌شود.



شکل ۱- لوگوی جدید اتحادیه Wi-Fi

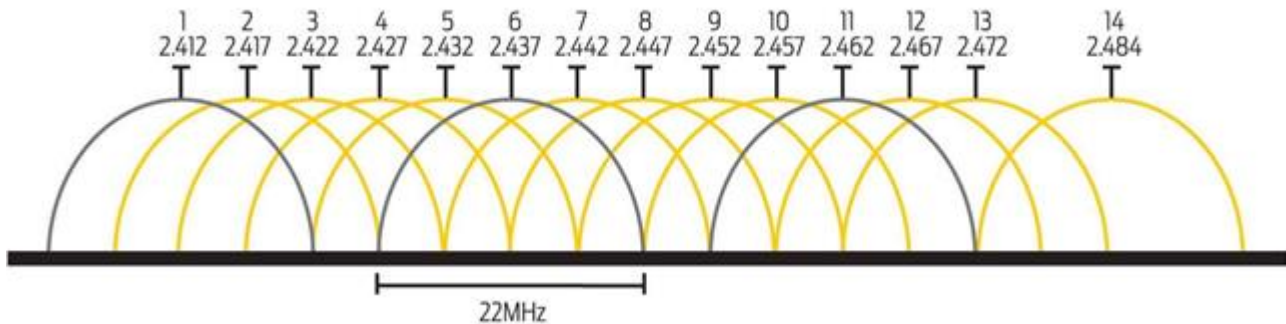
در جدول زیر انشعابات پرکاربرد استاندارد ۸۰۲،۱۱ را مشاهده می کنید:

جدول ۱- انواع مختلف استانداردهای 802.11

استاندارد	سال انتشار	باند فرکانسی برحسب گیگاهرتز (GHz)	پهنای باند برحسب مگاهرتز (MHz)	مدولاسیون	نوع فناوری آنتن	بیشترین سرعت انتقال اطلاعات
822.11	1997	2.4	20	DSSS, FHSS	N/A	2Mbps
822.11b	1999	2.4	20	DSSS	N/A	11Mbps
822.11a	1999	5.8	20	OFDM	N/A	54Mbps
822.11g	2003	2.4	20	DSSS, OFDM	N/A	54Mbps
822.11n	2009	2.4, 5.8	20, 40	OFDM	MIMO تا چهار آنتن	600Mbps
822.11ac	2013	2.4, 5.8	40, 80, 160	OFDM	MIMO, MU-MIMO تا هشت آنتن	6.93Gbps

۲- کانال های 802.11

امواج بی سیم برای انتقال خود باید از کانال های وایرلس استفاده کنند که دستگاه های وایرلس ۱۴ کانال را برای این کار مشخص کرده اند که هر کانال دارای قدرت ۲۰ مگاهرتز می باشند.



شکل ۲- کانال های شبکه وایرلس

بسیاری از مسیر یاب های بی سیم در بازه ای از ۲۴۰۰ تا ۲۵۰۰ مگاهرتز فعال می باشند و این بازه ۱۰۰ مگاهرتزی به ۱۴ کانال که هر کدام دارای ۲۰ مگاهرتز قدرت هستند تقسیم بندی می شوند که این امر باعث می شود که کانال های ۱ و ۶ و ۱۱ باهم همپوشانی (Overlapping) داشته باشند. این کانال ها ممکن است توسط سایر دستگاه های دیگر که دارای فناوری 802.11 می باشند نیز از همان کانالی استفاده کنند که شما نیز از آن استفاده می نمایید که با تغییر کانال به صورت دستی شما می توانید سرعت بهتری در انتقال اطلاعات از طریق شبکه بی سیم داشته باشید.

۳- انواع حالت‌های Wifi

فناوری Wifi دارای ۶ حالت مختلف است، که هر کدام دارای کاربردهای خاص خود می‌باشند.

۱-۳ **حالت Master:** این حالت که بانام‌های نقطه دسترسی و حالت سازمانی نیز از آن اسم برده می‌شود که یک سرویس AP مرسوم،

محسوب می‌شود. کارت وایرلس یک شبکه بانام خاص که همان SSID است را ایجاد می‌کند که دارای کانال و سایر خدمات معمول یک AP را ارائه می‌دهد. در این حالت کارت شبکه می‌تواند فقط با سایر کارت‌های دیگر که به آن وصل هستند یا آن‌ها را مدیریت می‌کند ارتباط ایجاد کند.

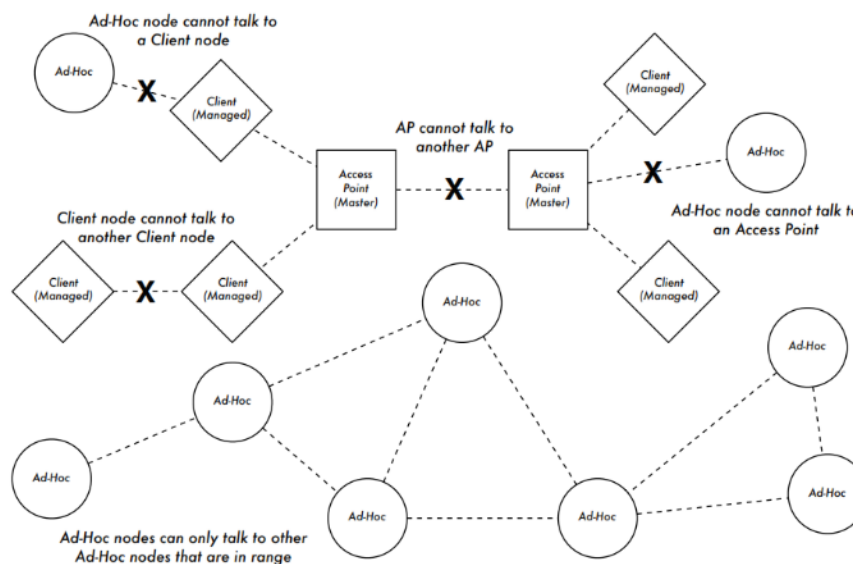
۲-۳ **حالت Managed:** از این حالت نیز بانام حالت سرویس گیرنده اسم برده می‌شود. کارت‌های شبکه در حالت مدیریت شده می‌توانند

به یک شبکه که توسط AP یا کارت در حالت Master ایجاد شده است ارتباط برقرار کنند و کانال خود را جهت مطابقت با آن‌ها به صورت خودکار تغییر دهند. این گونه کارت‌های به طور مستقیم نمی‌توانند با یکدیگر ارتباط برقرار کنند بلکه برای برقراری ارتباط نیاز به یک AP دارند.

۳-۳ **حالت Ad-hoc:** در این حالت در زمانی که هیچ گونه AP یا Master وجود نداشته باشد خود یک ارتباط چند نقطه به چند نقطه

را ایجاد می‌کند. در حالت Ad-hoc هر کارت شبکه به صورت مستقیم با همسایگان خود در ارتباط است. گروه باید در محدوده‌ی

یکدیگر باشند تا بتوانند باهم ارتباط برقرار کنند همچنین باید بر روی نام شبکه و کانال نیز به توافق برسند.

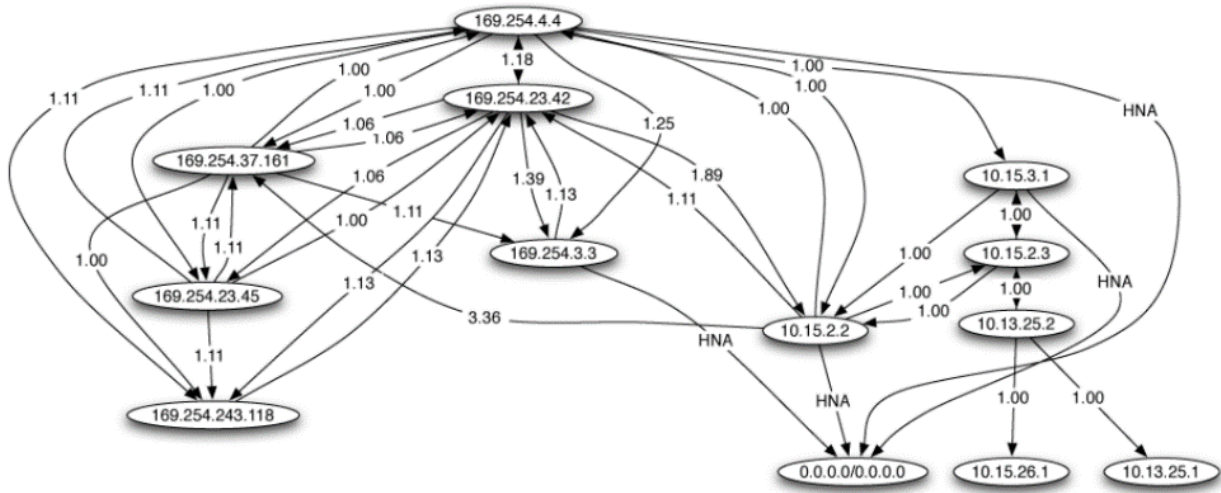


شکل ۳ - Nodeها در شبکه Ad-Hoc فقط می‌توانند با سایر nodeها در ارتباط باشند.

۴-۳ **حالت Monitoring:** از این حالت جهت گوش دادن غیرفعال و نظارت بر روی ترافیک موجود در کانال خاص استفاده می‌شود.

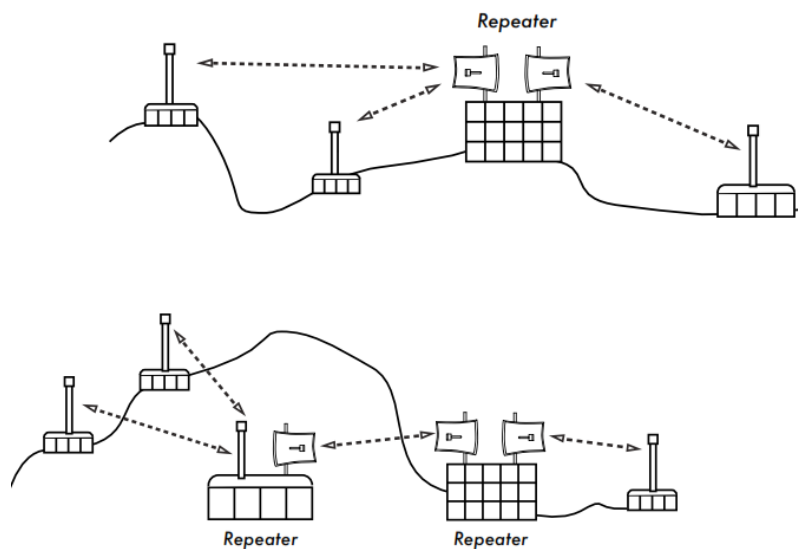
از این حالت برای ارتباطات عادی مورد استفاده قرار نمی‌گیرد بلکه مدیران شبکه از این حالت جهت تجزیه و تحلیل مشکلات داخل شبکه وایرلس و طیف استفاده از شبکه محلی استفاده می‌کنند.

۳-۵- Mesh network/cloud: شبکه‌های مش (با استفاده از تجهیزات 802.11) اساساً یک گروه از رادیوهایی است که در حالت Ad-hoc با استفاده از مسیریابی خاص عمل می‌کنند و باهم در ارتباط هستند. بسیاری از پروتکل‌های مسیریابی مش مانند OLSR ممکن است به هر شبکه‌ی فیزیکی مانند شبکه‌هایی که در حالت Master یا Managed و حتی شبکه‌های اترنت متصل شوند.



شکل ۴ - تصویری از شبکه مش

۳-۶- Repeaters: تکرارکننده سیگنال حالتی است که شما می‌توانید به‌وسیله آن سیگنال‌های مسیریاب یا اکسس پوینت اول را تقویت کنید. برای مثال فرض کنید در یک ساختمان هستید و این ساختمان ۲۰۰ متر است اما مسیریاب شما بیشتر ۱۰۰ متر توانایی سیگنال دهی ندارد برای رفع این مشکل درجایی که سیگنال ضعیف می‌شود می‌توان یک Repeater گذاشت تا سیگنال‌های ضعیف تقویت شوند و بتواند وسعت بیشتری از منطقه را تحت پوشش قرار دهد.



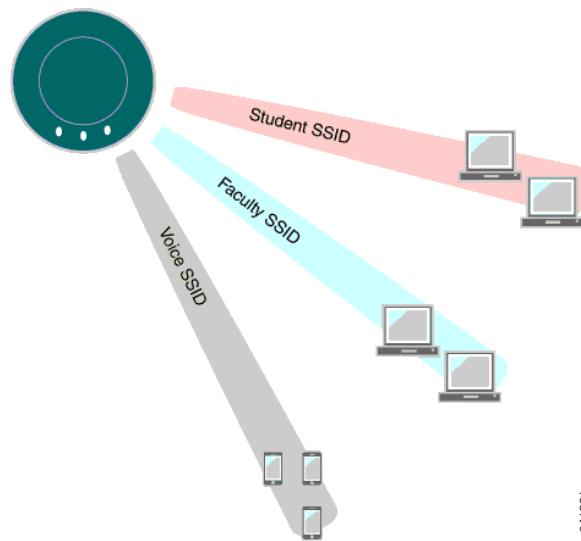
شکل ۵ - با استفاده از Repeater می‌توانید سیگنال‌های داخلی شبکه را تقویت کنید.

۴- نام شبکه‌های وایرلس

شبکه‌های وایرلس در پایه سیستم‌های پیچیده‌ای می‌باشند امکان انتخاب آن‌ها برای کاربران به‌سادگی وجود ندارد به همین دلیل برای قسمت‌های مختلف و ارتباط با آن‌ها نام‌گذاری‌های مختلفی انجام شد که در زیر به آن‌ها اشاره می‌کنیم.

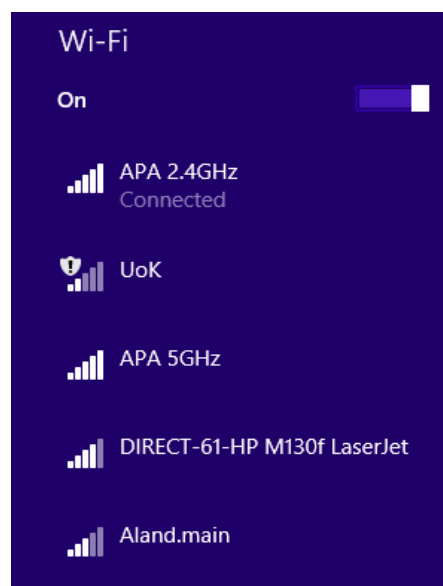
۴-۱- SSID

SSID مخفف Station Set Identifier است که نام شبکه‌های بی‌سیم است که توسط AP تعریف می‌شود تا کاربران بتوان جهت اتصال به شبکه به آن وصل شوند. با استفاده از SSID می‌توانیم شبکه‌ی خود را از سایر شبکه‌ها جدا کنیم و شبکه‌ی خصوصی خود را ایجاد کنیم.



شکل ۶- SSID جهت شناسایی شبکه مور نظر در میان سایر شبکه‌ها است.

در شکل بالا ۳ نوع SSID که هرکدام برای گروهی خاصی ایجاد شده است را می‌بینید. صورتی که شما بر روی ایکن WIFI کلیک کنید فهرستی از SSID های مختلف ظاهر می‌شد که شما می‌توانید شبکه‌ی موردنیاز خود را از طریق SSID تشخیص دهید.



شکل ۷- فهرستی از SSID های اطراف

۲-۴- BSSID چیست؟

BSSID مخفف عبارت Basic Service Set Identifier است که وظیفه‌ی آن تنظیم SSID است که در اصل پایه و اساس تنظیم این شناسه است.

روش تشخیص یک AP از طریق SSID آن‌ها نیست بلکه از طریق مک آدرس دستگاه است که این مک آدرس همان BSSID است و نهایتاً به SSID ترجمه می‌شود مانند سرویس DNS در وب که ایپی را به نام دامنه تبدیل می‌کند. با این تفاوت که امکان وجود دو AP در یک محیط وجود دارد چون دیوایس شما BSSID را می‌شناسد و SSID فقط یک نام برای کاربران است.

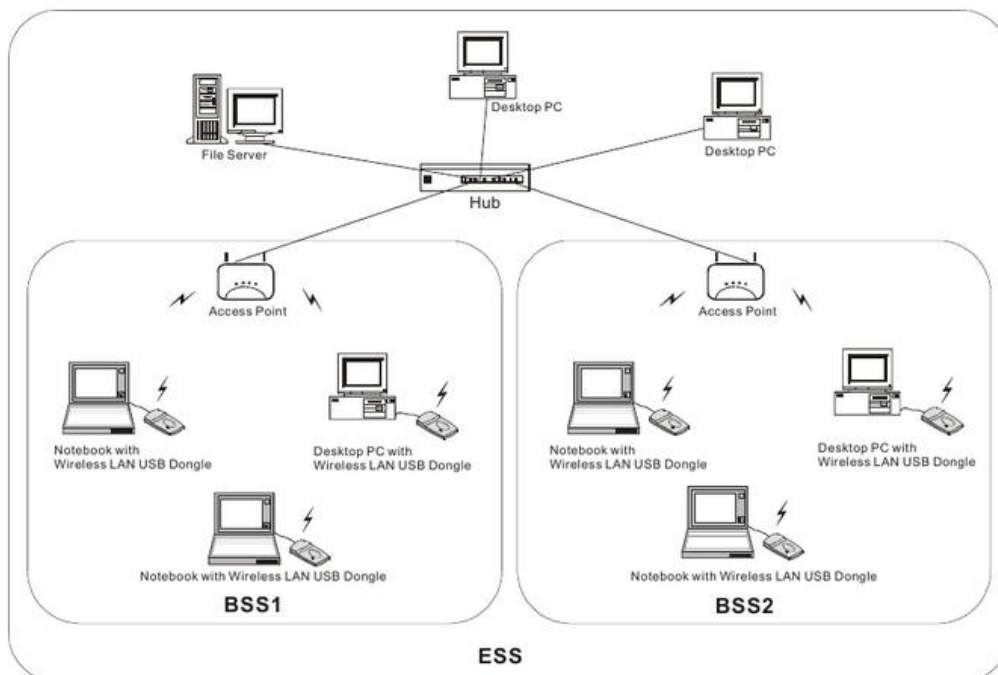
```

Select Windows PowerShell
PS C:\Users\I4tr0d3ctism> netsh wlan show interfaces
There is 1 interface on the system:
Name                : Wi-Fi
Description         : Intel(R) Dual Band Wireless-N 7260
GUID                : 28bc8b83-5e60-40ab-b930-323109b4e64d
Physical address    : ac:7b:a1:c4:f9:e6
State               : connected
SSID                : APA 2.4GHz
BSSID              : 1c:5f:2b:ff:a6:4c
Network type       : Infrastructure
Radio type         : 802.11n
Authentication     : WPA2-Personal
Cipher             : CCMP
Connection mode    : Profile
Channel            : 1
Receive rate (Mbps) : 144
Transmit rate (Mbps) : 144
Signal             : 83%
Profile            : APA 2.4GHz
Hosted network status : Not started
    
```

شکل ۸ - در ویندوز می‌توان BSSID را با استفاده از فرمان Netsh به دست آورد.

۳-۴- ESSID چیست؟

ESSID مخفف Extended Service Set Identifier است. ESS (extended service set) به مجموعه‌ای از basic service set (BSS) یا شبکه‌های وایرلسی اطلاق می‌شود که دارای Service set identification (SSID) های مختلف می‌باشند. به مجموعه SSID هایی که در داخل یک شبکه ESS وجود دارد را ESSID می‌نامند.



شکل ۹- شکل کلی شبکه ESS

۵- آنتن مناسب در آزمون نفوذ وایرلس

یکی از مباحث بسیار مهم و حیاتی در آزمون نفوذ به شبکه داشتن یک آنتن مناسب است که از طریق آن بتوان به راحتی به شبکه دسترسی پیدا کرد. آنت باید حالات مختلف مخصوصاً حالت Monitoring و pocket injection را با سرعت بالا پشتیبانی نماید. در زیر به معرفی انواع آنتن‌های شبکه‌های وایرلس می‌پردازیم:

۵-۱- آنتن جهت‌دار (Directional)

آنتن جهت‌دار برای انتشار (Broadcast) و گرفتن امواج رادیویی از یک جهت بکار می‌رود. به منظور افزایش کارایی انتقال و دریافت، آنتن‌های جهت‌دار طوری طراحی شده‌اند که در جهت‌های نزدیک به هم در مقایسه با سایر جهات به صورت مؤثر و کارا فعالیت کنند. این قابلیت باعث کاهش تداخلات نیز می‌شود.

۵-۲- آنتن چند جهته (Omni-Directional)

آنتن‌های چند جهته انرژی الکترومغناطیس را در تمام جهات و به صورت منظم از خود ساطع می‌کنند. آن‌ها معمولاً امواج قدرتمند یکسانی را در دو بعد از خود انتشار می‌دهند، اما این قدرت به اندازه‌ی حالت سه‌بعدی نیست. بهترین مثال برای آنتن‌های چندجهته، آنتن‌های مورد استفاده در ایستگاه‌های رادیویی هستند. این آنتن‌ها برای انتقال سیگنال‌های رادیو مؤثر هستند چراکه گیرنده‌ی امواج ممکن است متحرک باشد. در نتیجه رادیو می‌تواند سیگنال‌هایش را در جهتی برخلاف جهت آنتن دریافت کند.

۵-۳- آنتن شبکه‌ی سهمی‌وار

این آنتن‌ها بر اساس قاعده‌ی دیش‌های ماهواره‌ای کار می‌کنند. این نوع از آنتن‌ها یک دیش نصفه دارند و دارای یک شبکه که با استفاده از کابل آلومینیومی ایجاد شده است هستند. این آنتن‌های شبکه‌ای سهمی‌وار با استفاده از اصل پرتوی رادیویی متمرکز شده می‌توانند انتقال وای فای را به فواصل بسیار دور انجام دهند. اساساً این نوع از آنتن‌ها برای انتقال سیگنال‌های ضعیف رادیویی از میلیون‌ها کیلومتر دورتر از زمین بکار می‌روند.

۵-۴- آنتن Yagi

یاگی یک آنتن غیر جهت‌دار است که در ارتباطات یک باند فرکانسی ۱۰ مگاهرتز به VHF و UHF مورد استفاده قرار می‌گیرد. این آنتن‌ها به آنتن‌های Yagi Uda نیز مشهور هستند.

۵-۵- آنتن دوقطبی

یک دوقطبی، یک هادی الکتریکی مستقیم است که نصف طول موج را اندازه‌گیری می‌کند.

۶- چیپست مناسب

موضوع مهم در آزمون نفوذ شبکه‌های بی‌سیم لیست چیپست‌هایی است که توسط سیستم‌عامل‌ها و برنامه‌های آزمون نفوذ از آن‌ها استفاده شده است که معمولاً قوی‌ترین نوع چیپست‌ها نیز می‌باشند. در زیر فهرستی از چیپست‌هایی که توسط سیستم‌عامل kali مورد پشتیبانی می‌شود و همچنین دارای حالت‌های injection و monitoring می‌باشند را معرفی می‌کنیم.

•Atheros AR9271

- Ralink RT3070
- Ralink RT3572
- Realtek 8187L (Wireless G adapters)
- Realtek RTL8812AU
- Ralink RT5370N

این چیس‌ت‌ها دارای قدرت خوبی برای عملیات آزمون نفوذ است و در لیست زیر بهترین کارت‌های شبکه در عملیات آزمون نفوذ را معرفی کرده‌ایم.

جدول ۲ - فهرستی از بهترین کارت‌های وایرلس برای آزمون نفوذ

Antenna	Pros	Cons
<u>Alfa AWUS036H</u>	OS Compatibility, Decent Gain, Stable	Large, Obvious, Medium-Poor Range
<u>Turbotenna-802.11n</u> <u>Directional-Yagi-antenna</u>	OS Compatibility, Extremely High Gain, Sensitive	Large, Obvious, Directional, N-Only
<u>TP-LINK TL-WN722N</u>	OS Compatibility, Price, Size, B/G/N	Poor gain (micro version even less)
<u>Alfa AWUS036NEH</u>	Small, Price, OS Compatibility	Shorter range
<u>Alfa AWUS036NHA</u>	OS Compatibility, Speed, B/G/N	Smaller range, size



شکل ۱۰- بهترین کارت‌های شبکه جهت آزمون نفوذپذیری شبکه‌های وایرلس

۷- فریم‌های شبکه 802.11

بیشتر افراد به‌اشتباه گمان می‌کنند که شبکه‌های wireless مانند 803.2 LAN ها کار می‌کنند. در صورتی که LAN های 802.3 از آدرس‌های MAC استفاده می‌کنند، اما LAN های وایرلس از ساختار فریم 802.11 استفاده می‌نمایند.

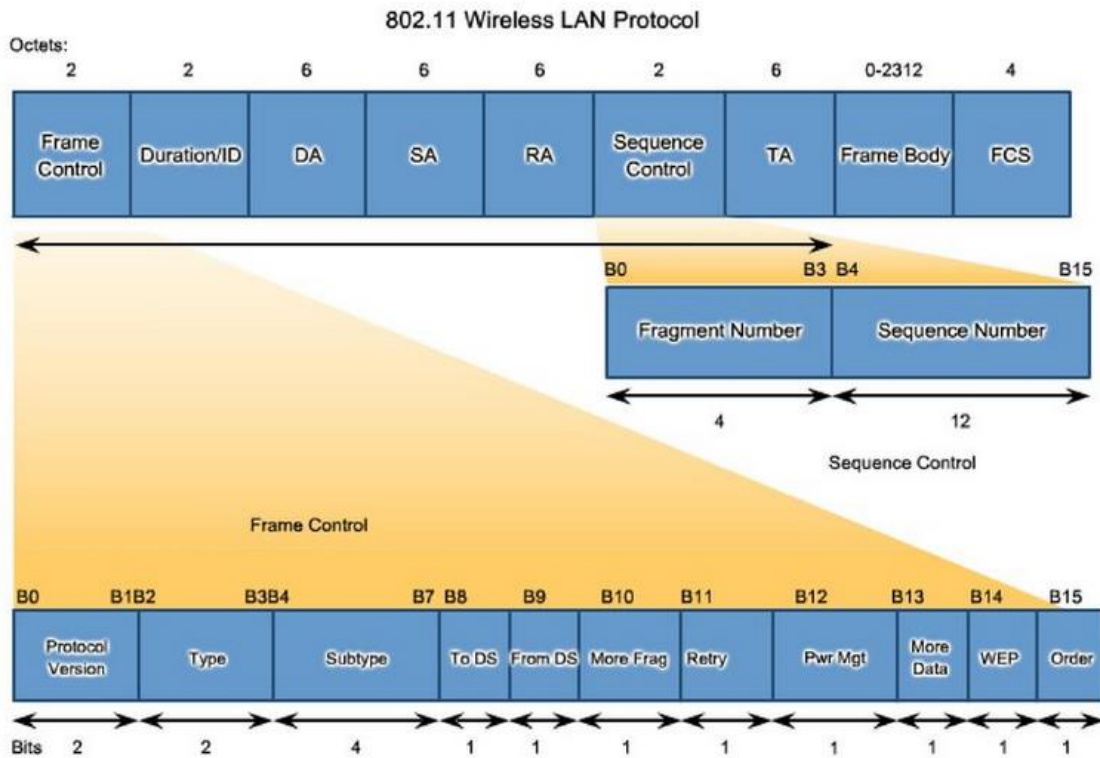
در پروتکل 802.11 ۳ نوع فریم وجود دارد:

۱- فریم داده (Data Frames): فریم‌هایی که حاوی داده‌های اصلی می‌باشند.

۲- فریم کنترلی (Control Frames): برای تائید (acknowledge) اینکه فریم‌های دیتا (data frames) دریافت شده‌اند.

۳- فریم‌های مدیریتی (Management Frames): برای پیوستن یا ترک کردن یک سلول وایرلس به کار می‌رود. این نوع

فریم شامل درخواست association، پاسخ به آن، درخواست دوباره و ... است.



شکل ۱۱- فریم‌های مدیریتی 802.11

در زیر به شرح مختصری درباره فریم‌ها می‌پردازیم:

۱-۷- فریم کنترلی Frame Control

این فریم خود از ۹ زیر فیلد فرعی تشکیل شده است. از طریق این فیلد نوع فریم مشخص و مقداری اطلاعات کنترلی برای پردازش صحیح بسته و تفسیر دقیق آدرس‌ها به مقصد ارائه می‌شود. زیر فیلدهای فیلد Frame Control در زیر مشخص شده است:

- زیر فیلد Protocol version: این فیلد دو بیتی، شماره‌ی نسخه پروتکل شبکه‌ی بی‌سیم را تعیین می‌کند.
- زیر فیلد Type: نوع فریم را مشخص می‌کند: که مقدار ۰۰ فریم‌های مدیریتی، ۰۲ فریم‌های کنترلی و ۱۰ فریم‌های داده است.
- زیر فیلد Subtype: نوع فریم مدیریتی یا کنترلی را مشخص می‌کند.
- زیر فیلدهای To DS و From DS: به همراه چهار فیلد آدرس، در آدرس‌دهی کاربرد دارند.

- زیر فیلد More Flag: مقدار ۱ بدین معناست که در ادامه فریم جاری بازهم قطعه دیگری خواهد آمد.
 - زیر فیلد Retry: مقدار ۱ بدین معناست که فریم جاری، یک فریم جدید نیست بلکه همان فریم قبلی است که به دلیل نرسیدن تأییدیه‌ی آن (ACK) از نو فرستاده شده است.
 - زیر فیلد Power mgt: مقدار ۱ تنظیم شده باشد بدین معناست که ایستگاه در حالت صرفه‌جویی توان قرار دارد.
 - زیر فیلد WEP: مقدار ۱ بدین معناست که بدنه‌ی فریم به روش RC4 رمزنگاری شده است.
 - زیر فریم Order: این بیت به گیرنده تفهیم می‌کند که دنباله‌ای از فریم‌ها که این بیت در آن‌ها ۱ است باید الزاماً به ترتیب و پشت سر هم پردازش شوند.
- فیلد آدرس (۱ تا ۴): مکانیزم آدرس‌دهی در IEEE 802.11 در مقایسه با اترنت پیچیده‌تر است چراکه در شبکه‌های بی‌سیم وقتی مبدأ و مقصد در دو سلول متفاوت واقع‌اند فریم ارسالی یک ایستگاه باید از دو AP میانی می‌گذرد. بنابراین وجود چهار فیلد آدرس در هر فریم ضروری می‌نماید که یک جفت برای تعیین آدرس ایستگاه‌های نهایی مبدأ، و مقصد و یک جفت دیگر برای تعیین AP های میانی (در صورت نیاز). دو بیت پرچم To DS و From DS نیز برای تعیین نوع آدرس‌ها و تبیین عملکرد AP های میانی کاربرد دارد.
- فیلد FCS: در این فیلد چهار بیتی، کد کشف خطای کل فریم است که به روش CRC-32 محاسبه و درج می‌شود.
 - فیلد DATA: در این فیلد داده‌هایی قرار می‌گیرد که توسط لایه‌های بالایی جهت تحویل به یک مقصد خاص به سخت‌افزار شبکه‌ی بی‌سیم تسلیم شده است. در این فیلد حداقل صفر و حداکثر ۲۳۱۲ بایت داده قرار می‌گیرد. البته اگر نوع فریم، کنترلی یا مدیریتی باشد در بطن این فیلد داده‌های مرتبط با عملکرد آن فریم درج خواهد شد.

۲-۷- فریم‌های مدیریتی – پیوستن به شبکه و ترک آن (Management Frames)

فریم‌های مختلفی جهت مذاکره اولیه بین نودها و AP ها کاربرد دارد که به‌عنوان زیرمجموعه‌های فریم‌های مدیریتی محسوب می‌شوند که در زیر به معرفی آن‌ها می‌پردازیم.

جدول ۳ - انواع فریم‌های مدیریتی

نوع فریم	Subtype Bits
Association request	0000
Association response	0001
Reassociation request	0010
Reassociaiton response	0011
Probe request	0100
Probe response	0101
Beacon	1000
ATIM (Announcement traffic indication message)	1001

Disassociation	1010
Authentication	1011
Deauthentication	1100
Action	1101

۱-۲-۷- درخواست پیوستن به شبکه (Association request)

ایستگاه‌های سیار به محض آنکه وارد محدوده‌ی رادیویی یک AP می‌شوند بایستی قبل از هر کاری هویت و نیازمندی‌های خود را به AP معرفی کنند تا بتوانند از خدمات آن بهره برد. برای این کار: ایستگاه ابتدا فریم مدیریتی Probe Request را منتشر می‌کند. تمام APهایی که چنین فریمی را می‌شنوند بافریم Probe Request پاسخ می‌دهند. ایستگاه از بین APهایی که پاسخ داده‌اند یکی را با ارسال Association Request برمی‌گزیند. (ملاک انتخاب می‌تواند مقایسه‌ی سیگنال دریافتی از AP باشد) AP با فرستادن فریم Association Response پاسخ مساعد می‌دهد.

۲-۲-۷- ترک شبکه (Disassociation)

هرگاه یک ایستگاه (یا حتی یک AP) بخواهد به حضور خود در شبکه خاتمه بدهد با ارسال Disassociation این تصمیم را به آگاهی دیگران می‌رساند.

۳-۲-۷- فریم‌های مدیریتی - پیوستن مجدد به شبکه (Reassociation)

هرگاه ایستگاهی به سلول جدیدی وارد شود با ارسال این به AP واقع در سلول جدید اعلام حضور می‌کند. بدین ترتیب AP جدید از آدرس این ایستگاه مطلع شده و به AP قبلی او اعلام می‌کند که چنین ایستگاهی دیگر عضو او نیست. برای عملیات پیوستن مجدد به شبکه مراحل زیر دنبال می‌شود: ایستگاه با فریم مدیریتی Reassociation Request از AP سلول جدید تقاضای پیوستن مجدد می‌نماید. AP با ارسال فریم Reassociation Response جواب می‌دهد.

۴-۲-۷- احراز هویت (Authentication):

جهت جلوگیری از دسترسی ایستگاه‌های غیرمجاز به خدمات AP هر ایستگاه باید قبل از دریافت مجوز ارسال، هویت خود را اثبات نماید. این کار توسط فریم Authentication انجام می‌شود.

۵-۲-۷- لغو حضور و سلب هویت (Deauthentication)

هر ایستگاه باید قبل از خروج از شبکه حضور خود را لغو و هویت ثبت‌شده‌ی خود را سلب و بی‌اعتبار سازد. Deauthentication به همین منظور تولید و ارسال می‌شود.

۶-۲-۷- تبادل امن (Secure Communication)

جهت ارتباطی امن و مبتنی بر رمزنگاری یک یا چند فریم Authentication می‌فرستد. الگوریتم رمزنگاری بکار رفته عموماً RC4 است ولی به دلیل مشکلاتی که در این روش پیدا شد در محصولات جدید از الگوریتم AES استفاده می‌شود.

۳-۷- احراز هویت

ایستگاه‌ها موظفاند قبل از پیوستن به یک AP هویت خود را بر اساس مراحل زیر اثبات کنند. پس از آنکه ایستگاه سیار به حوزه پوشش یک AP وارد شد، آن AP بلافاصله یک فریم خاص به نام فریم چالش (Challenge) برای او می‌فرستد. این فریم عموماً حاوی داده‌هایی تصادفی است که در ارسال‌های متوالی هرگز تکراری نخواهند بود. ایستگاه سیار موظف است داده‌های درون فریم چالش را با کلید سری خود رمز کرده و برای AP پس بفرستد تا ثابت کند کلمه عبور خود را می‌داند.

AP فریم برگشتی ایستگاه سیار را گرفته و محتویات آن را کلید سری آن ایستگاه رمزگشایی کرده و آن را با داده‌های ارسالی خود مقایسه می‌نماید. اگر نتیجه درست بود طبعاً ایستگاه سیار راست می‌گوید! (AP کلید سری همه‌ی ایستگاه‌های مجاز را می‌داند). پس از اثبات هویت ایستگاه سیار، عضویت او در گروه مسجل خواهد شد و می‌تواند پس از پیوستن به AP از خدمات آن AP بهره بگیرد.

۴-۷- دعوت از ایستگاه‌ها با فریم (Beaconing)

هر AP به‌طور متناوب با ارسال فریم Beaconing از ایستگاه‌هایی که احتمالاً علاقه‌مند پیوستن به شبکه هستند دعوت به عمل می‌آورد. روال کار زیر است:
AP فریم Beacon ارسال می‌کند.
ایستگاهی که تمایل به پیوستن به شبکه دارد فریم Association Request را ارسال می‌کند.

۵-۷- گزارش در خصوص فریم‌های آماده ارسال (ATIM)

هرگاه ایستگاهی، چندین فریم بافر شده و آماده‌ی ارسال برای ایستگاه‌های دیگر داشته باشد می‌تواند با ارسال فریم مدیریتی ATIM به ایستگاه‌های دیگر در خصوص فریم‌های که در آینده دریافت خواهند کرد گزارش بدهد.

۶-۷- مکانیزم رومینگ یا Handover

به مکانیزمی که به ایستگاه‌های اجازه می‌دهد تا بتوانند به راحتی بین سلول‌ها حرکت کنند و بدون قطع ارتباط یا از دست رفتن داده‌ای از یک AP جدا شده و به یک AP جدید اصطلاحاً رومینگ گفته می‌شود.
در مکانیزم رومینگ ایستگاه می‌تواند تشخیص دهد که سلول او عوض شده است و باید AP خود را عوض کند برای این کار هر AP به‌طور متناوب فریمی به نام Beacon را در سلول تحت پوشش خود منتشر می‌کند. در این فریم اطلاعاتی در خصوص شناسنامه‌ی AP و پارامترهای لینک رادیویی درج شده است و ایستگاه‌های سیار دائماً این فریم‌ها را دریافت و تحلیل می‌کنند. هرگاه ایستگاهی از AP سلول فعلی خود دور و به یک AP در سلول مجاور نزدیک شود شدت سیگنال دریافتی از سلول قبلی، رو به ضعف می‌گذارد و در عوض سیگنال دریافتی از AP سلول مجاور قوت می‌گیرد. به عبارت فنی با دور شدن از یک AP، نسبت Signal to Noise Ratio رو به کاهش می‌گذارد و در عوض نسبت به Bit Error Rate افزایش خواهد یافت.
ایستگاه با شنود Beacon، پارامتر SNR یا BER آن را ارزیابی و سیگنال دارای SNR بیشتر و BER کمتر باشد را به‌عنوان سیگنال برگزیده انتخاب می‌کند.

پس از مراحل فوق هماهنگی‌های لازم برای تکمیل انتقال انجام می‌شود.

با استخراج مشخصات AP از درون فریم فانوس، یک فریم مدیریتی Authentication به‌سوی آن AP ارسال می‌شود. پس از تأیید هویت ایستگاه تازه‌وارد و اعلام موافقت، از طریق شبکه‌ی سیمی بین AP ها تغییر سلول این ایستگاه به AP قبلی وی اعلام شده و از اعضای گروه سلول قبلی حذف و سلب هویت می‌گردد. حال ایستگاه اجازه می‌یابد با ارسال فریم مدیریتی Reassociation به AP جدید متصل شده و از خدمات آن بهره بگیرد.

۸- رمزنگاری در شبکه‌های بی‌سیم و ضعف‌های امنیتی آن‌ها

رمزنگاری وایرلس فرایندی است در محافظت از شبکه وایرلس در برابر نفوذ مهاجمان که می‌تواند با نقض ترافیک فرکانس رادیویی (RF)، اطلاعات محرمانه و حساس موجود در شبکه را جمع‌آوری کنند. این نکته مروری خواهد داشت بر استانداردهای مختلف رمزنگاری وایرلس مثل WEP، WPA و WPA2. شدت حمله بر روی شبکه وایرلس روز به روز با گسترش استفاده آن، بیشتر می‌شود. بنابراین برای این فناوری نوظهور و جدید، شیوه‌های مختلف از الگوریتم‌های رمزنگاری ابداع شده است تا امنیت آن را بیش از پیش تأمین کرده باشند. هر کدام از این شیوه‌ها مزایا و معایب خاص خود را دارند. در زیر به بررسی هر کدام از این روش‌ها می‌پردازیم:

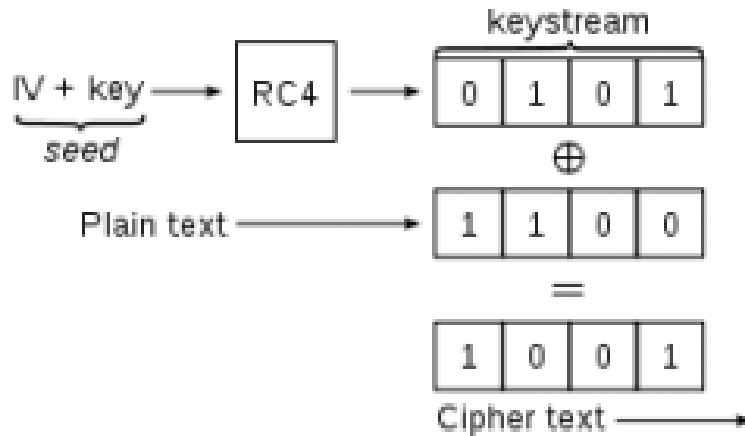
- **WEP:** پروتکل احراز هویت و رمزنگاری دیتا در سرویس‌گیرنده‌های شبکه وایرلس است؛ اما این شیوه قدیمی شده است و باینکه استاندارد اصلی امنیت در شبکه وایرلس محسوب می‌شود اما به راحتی قابل کرک شدن است.
- **WPA:** این شیوه یک پروتکل پیشرفته احراز هویت و رمزنگاری دیتا در سرویس‌گیرنده‌های شبکه وایرلس است که از رمزنگاری‌های TKIP، MIC و AES استفاده می‌کند. همچنین در این روش از رمزنگاری‌های ۴۸-bit IV، ۳۲-bit CRC و TKIP برای تأمین امنیت وایرلس استفاده می‌شود.
- **WPA2:** این روش از AES (128) و CCMP برای رمزگذاری دیتای وایرلس استفاده می‌کند.
- **WPA2 Enterprise:** این روش استانداردهای AES را با رمزنگاری WPA یکپارچه کرده است.
- **TKIP:** یک پروتکل امنیتی که در WPA و به‌عنوان جایگزینی برای WEP مورد استفاده قرار می‌گیرد.
- **AES:** یک رمزنگاری از نوع کلید متقارن است که در WPA2 و به‌عنوان جایگزینی برای TKIP مورد استفاده قرار می‌گیرد.
- **EAP:** از روش‌های مختلف احراز هویت مثل Token card، Kerberos، Certificate و غیره استفاده می‌کند.
- **LEAP:** یک پروتکل اختصاصی احراز هویت شبکه وایرلس که توسط سیسکو ایجاد شده و مورد استفاده است.
- **RADIUS:** یک سیستم احراز هویت مرکزی و مدیریت اعتبار است.
- **۸۰۲٫۱۱:** یکی از استانداردهای IEEE که مکانیزم‌های امنیتی را برای شبکه‌های وایرلس ۸۰۲٫۱۱ مشخص می‌کند.
- **CCMP:** از کلیدهای ۱۲۸ بیتی به همراه یک حامل اولیه ۴۸ بیتی (IV) برای تشخیص انتشار استفاده می‌کند.

۸-۱- رمزنگاری WEP چیست؟

WEP (مخفف Wireless Encryption Protocol یا Wired Equivalent Privacy) یکی از الگوریتم‌های امنیتی در شبکه‌های بی‌سیم ۸۰۲٫۱۱ است. WEP چندان امن نیست و قابل نفوذ است؛ با این حال در تمامی دستگاه‌های بی‌سیم پشتیبانی می‌شود. بزرگترین ضعف WEP استفاده از کلید ثابت (Static) است. به این معنی که همه‌ی کاربران با رمز یکسان به دستگاه بی‌سیم متصل می‌شوند و تمامی بسته‌ها فقط با یک کلید رمزگذاری می‌گردند. به این ترتیب با استراق سمع، بسته‌های WEP کافی برای کشف کلید وجود دارد. فرمت کلید در WEP

کلید WEP می‌تواند ۶۴ یا ۱۲۸ بیتی باشد که به ترتیب شامل ۱۰ و ۲۶ رقم هگزا دسیمال است. یعنی برای کلید ۱۲۸ بیتی باید ۲۶ رقم هگزا دسیمال وارد نمود (هر رقم هگزا دسیمال یک عدد بین ۰ تا ۹ یا یک حرف از A تا F میتواند باشد).

ضمناً در بعضی دستگاه ها می توانیم به جای ارقام هگزا دسیمال یک رشته متنی وارد کنیم ولی باز هم این کاراکترها به مقادیر معادل اسکی (ASCII) تبدیل می شوند. پس واضح است که برای کلید ۶۴ بیتی یک رشته ی ۵ کاراکتری و برای کلید ۱۲۸ بیتی یک رشته ی ۱۳ کاراکتری می توان وارد نمود (هر کاراکتر در استاندارد ASCII با دو رقم هگزا تعریف می شود).



شکل ۱۲- رمزنگاری RC4 در WEP

در این روش برای Authentication کردن دو راه وجود دارد:

احراز هویت بدون رمزنگاری (Open System Authentication)

در این روش سرویس گیرنده نیازی به تهیه یک مجوز برای ارتباط با Access Point ندارد. در حقیقت هیچ Authentication صورت نمی گیرد. سرویس گیرنده بدون اینکه هویتش تأیید شود می تواند به شبکه متصل شود اما اگر کلید درست را نداشته باشد نمی تواند بسته هایی که رمز شده را باز کند.

احراز هویت با کلید مشترک (Shred Key Authentication)

در این روش چهار مرحله برای احراز هویت سرویس گیرنده وجود دارد.

۱. در اولین گام سرویس گیرنده درخواست احراز هویت خود را برای Access Point ارسال می کند.
۲. در گام دوم Access Point با ارسال بسته ای حاوی اطلاعاتی ساده به سرویس گیرنده سعی می کند سرویس گیرنده را به چالش بکشد.
۳. در این مرحله سرویس گیرنده محتویات بسته را با کلید WEP رمز کرده و برای Access Point ارسال می کند.

و در نهایت Access Point بسته دریافتی را رمزگشایی کرده و در صورتی که محتویات بسته همان محتویات ارسالی خودش باشد هویت سرویس گیرنده تأیید می شود. در نگاه اول تأیید هویت به روش دوم بهتر است اما در حقیقت این طور نیست و تأیید هویت کاربر در روش اول بهتر است. البته باید توجه کنید که هیچ کدام از این دو روش امنیت بالایی را برای شبکه شما فراهم نمی کنند.

۸-۲- ضعف‌های امنیتی WEP

در فهرستی از ضعف‌های امنیتی پروتکل WEP به اختصار جمع‌بندی شده است.

جدول ۴ - آسیب پذیری‌های موجود در WEP

توضیحات	بحث امنیت و آسیب‌پذیری
ویژگی‌های امنیتی در برخی موارد ضعیف هستند و تا زمانی که تغییر محل داده نشوند فعال نمی‌شوند. معمولاً در هنگام نصب نیز توسط کاربران فعال نمی‌شوند. امنیت کم بهتر از نبود آن است.	در اغلب موارد ویژگی‌های امنیتی در هنگام تولید توسط شرکت‌های تولیدکننده محصولات بی‌سیم فعال نمی‌شود
تعداد بیت‌های IV برابر ۲۴ است که باعث تکرار کلید جاری تولید شده می‌شوند. این تکرار رمزگشایی داده را برای یک نفوذگر ماهر آسان می‌کند.	IVها کوتاه یا ایستا هستند.
کلیدهای ۴۰ بیتی برای سیستم‌های امنیتی کافی نیستند. به‌طور کلی و استاندارد، باید اندازه کلید بیشتر از ۸۰ بیت باشد. احتمالاً کشف کلیدهای طولانی در اثر یک حمله BruteForce بسیار کمتر است.	کلیدهای رمزنگاری کوتاه است.
احتمال کشف کلیدهای اشتراکی توسط یک سیستم بسیار زیاد است. تسلط به مکانیزم‌های بنیادی رمزنگاری مخصوص یک سیستم، تا حد زیادی به کلیدهای محرمانه وابسته است.	کلیدهای رمزنگاری اشتراکی هستند.
کلیدهای رمزنگاری باید به‌کرات جهت جلوگیری از حملات BruteForce تغییر کنند.	اغلب کلیدهای رمزگذاری به‌طور خودکار به‌روزرسانی نمی‌شوند.
ترکیب بیت‌های کلید ۲۴ بیتی با IV یک تهدید محسوب می‌شود. این امر سبب هدایت یک حمله مؤثر به‌منظور دستیابی به کلید می‌شود. اغلب برنامه‌های کاربردی دیگر که از RC4 استفاده می‌کنند، ضعف‌های موجود در آن را افشا نمی‌کنند. زیرا آن‌ها بیت‌های کلید را فاش نمی‌کنند و همچنین زمان‌بندی کلید را برای هر بسته تغییر نمی‌دهند. این حمله اطلاعات مفیدی در دسترس یک نفوذگر ماهر قرار می‌دهد.	زمان‌بندی کلید در RC4 ضعیف است و از آن به‌طور غیر مقتضی در WEP استفاده می‌شود.
کد CRC32 و دیگر کدهای مسدودکننده خطی جهت تأمین بی‌عیب و نقصی در رمزنگاری کافی نیستند. تغییر در محتویات یک پیام امکان‌پذیر است. کدهای خطی جهت محافظت در مقابل حملات دقیق بر روی داده‌ها کافی نیستند. حفاظت از رمزنگاری نیازمند جلوگیری از انجام حملات پیش‌بینی‌شده و عمدی است. بهره‌گیری از پروتکل‌های که از مکانیزم‌های رمزنگاری استفاده نمی‌کنند، اغلب موارد به حملات علیه رمزنگاری کمک می‌کنند.	بی‌عیب و نقصی بسته ناچیز است.
تنها شبکه احراز هویت می‌شوند. یک دستگاه رپوده شده به‌راحتی می‌تواند به شبکه دسترسی پیدا کند.	احراز هویت کاربر انجام نمی‌شود.
سیستم‌های بر پایه تشخیص هویت در شبکه‌ها و سیستم‌های بی‌سیم، به‌طور عادی دارای آسیب‌پذیری‌های جزئی زیادی هستند.	احراز هویت غیرفعال است: تنها شناسایی ساده SSID انجام می‌شود.
پاسخ مذاکره یک‌طرفه در احراز هویت، عامل اساسی در ایجاد حملات MITM است. احراز هویت دوطرفه نیازمند آماده‌سازی‌های اولیه جهت بازبینی و تصدیق کاربران و شبکه‌های قانونی است.	۱۰. احراز هویت تجهیزات بر اساس پاسخ مذاکره ساده کلید اشتراکی است.

۸-۳- WPA یا Wi-Fi Protected Access :

WPA به‌عنوان جایگزین WEP منتشر شد. این الگوریتم در سال ۲۰۰۳، یعنی یک سال قبل از اعلام از دور خارج شدن استاندارد WEP، تصویب شد. WPA-PSK از رایج‌ترین پیکریندی‌های WPA است. کلیدی که به‌وسیله WPA استفاده می‌شود، ۲۵۶ بیتی است.

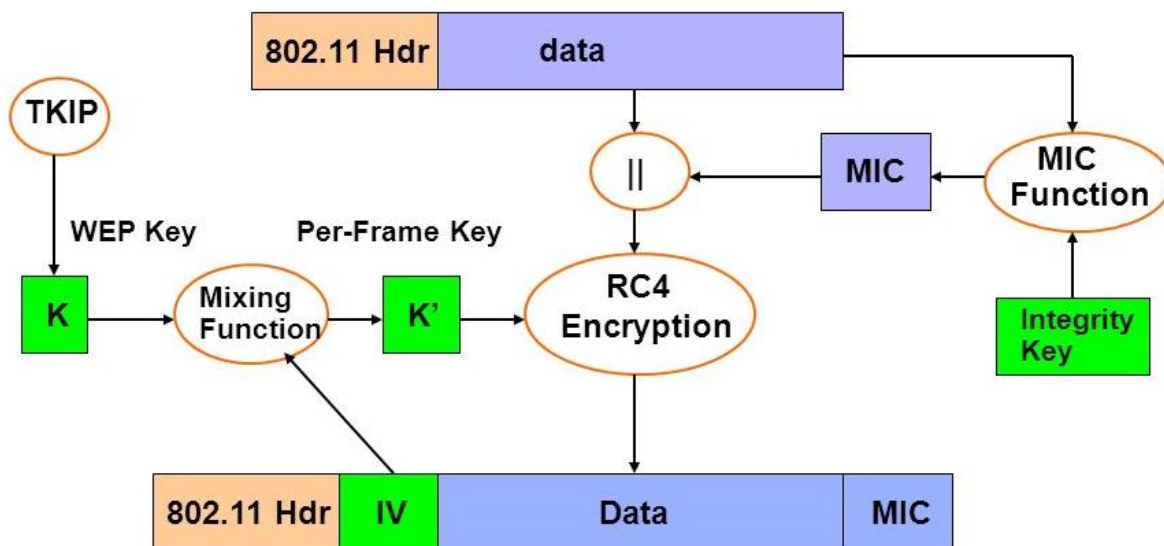
برخی از تغییرات قابل‌توجه در WPA شامل بررسی یکپارچگی پیام، و پروتکل تمامیت کلید موقت (TKIP) است. TKIP بعدها توسط استاندارد رمزنگاری قدرتمند AES جایگزین شد.

باوجوداینکه WPA پیشرفت‌های قابل‌توجهی نسبت به WEP کرده بود، از آسیب‌پذیری در امان نماند. TKIP، کامپوننت مرکزی WPA، به‌گونه‌ای طراحی شده بود که به‌راحتی از طریق به‌روزرسانی میان‌افزار (Firmware)، بتواند روی دستگاه‌های موجودی که WEP فعال دارند، اجرا شود. به‌این‌ترتیب مجبور بود المنت‌های خاصی که توسط WEP استفاده می‌شدند و نفوذپذیر بودند را بازیابی کند. به WPA هم مانند WPE حمله شد، اما مستقیم به خود الگوریتم حمله انجام نشد.

۸-۴- WPA چگونه کار می‌کند؟

در زیر به چگونگی کارکرد پروتکل رمزنگاری WPA می‌پردازیم.

- برای رمزنگاری مؤثر payload، رمزنگاری WPA مراحل زیر را انجام می‌دهد
- کلید موقت رمزنگاری، آدرس انتقال و شمارنده TKIP به‌عنوان ورودی‌های الگوریتم RC4، باعث ایجاد یک جریان کلید می‌شوند. (MSDU) MAC Service Data Unit و MIC توسط الگوریتم Michael با یکدیگر ترکیب می‌شوند.
- ترکیب حاصله از MSDU و MIC به‌منظور ایجاد MAC Protocol Data Unit (MPDU)، بخش بخش (فراگمنت) می‌شوند.
- یک مقدار ۳۲ بیتی برای بررسی یکپارچگی (ICV) برای MPDU محاسبه می‌شود.
- ترکیب MPDU و ICV به همراه یک جریان کلید برای رمزنگاری دیتا بکار می‌رود.
- IV به دیتای رمز شده جهت تولید فریم مک اضافه می‌شود.



شکل ۱۳ - نحوه‌ی کار پروتکل امنیتی WPA

۸-۵- WPA2 چیست؟

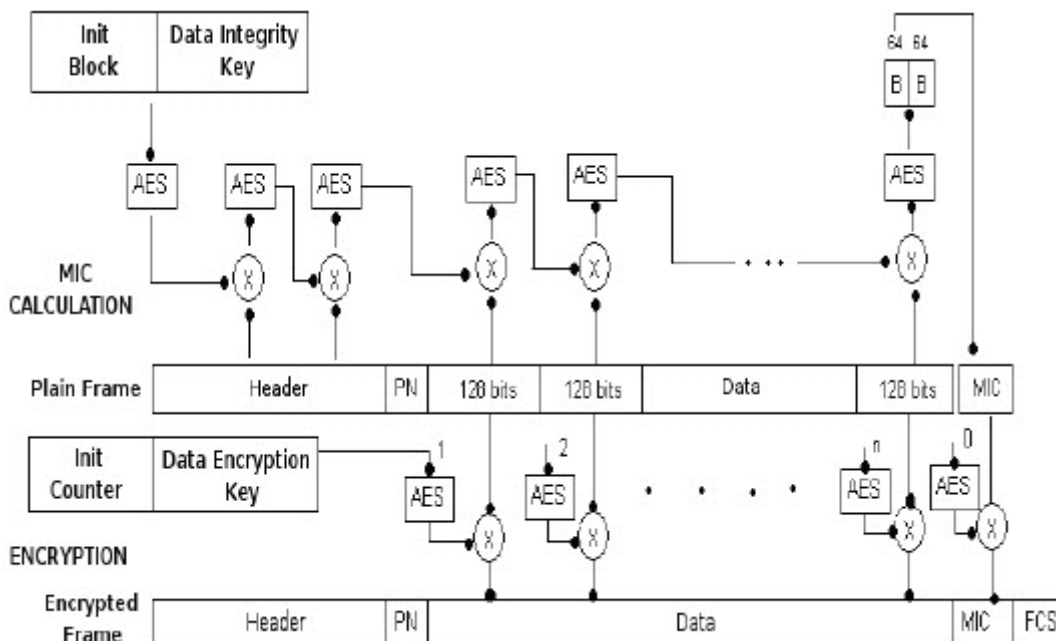
پروتکل امنیتی (WPA2 (Wi-Fi Protected Access II) پروتکلی است که کاملاً با استاندارد 802.11i همخوانی و همسویی دارد. این پروتکل بیشتر خصوصیات امنیتی را که WPA پشتیبانی نمی‌کند را تحت پوشش خود قرار می‌دهد و در مقایسه با آن حفاظت از اطلاعات و کنترل دسترسی قوی‌تر دارد. این پروتکل امنیت را با سطح بالایی در شبکه ایجاد می‌کند بنابراین فقط کاربران مجاز می‌توانند به آن دسترسی داشته باشند WPA2. توسط الگوریتم رمزنگاری AES پیاده‌سازی شده است و درجه امنیتی که ایجاد می‌کند مطابق با سطح دولتی است. این الگوریتم دارای دو حالت مختلف است:

WPA-Personal: این نسخه از پسوردهای در نظر گرفته شده (Pre-shared key)، (PSK) برای محافظت از دسترسی‌های غیرمجاز به شبکه استفاده می‌کند. در حالت PSK، هر دستگاه در شبکه وایرلس ترافیک را با استفاده از کلید ۲۵۶ بیتی رمزنگاری می‌کند که می‌تواند در قالب ۸ تا ۶۳ کاراکتر ASCII وارد شود.

WPA-Enterprise: در این روش کاربر شبکه از طریق یک سرور تائید هویت می‌شود. برای این کار از EAP و یا RADIUS برای احراز هویت مرکزی سرویس گیرنده و از شیوه‌های مختلف مثل Token card، Kerberos، Certificate و ... برای این کار استفاده می‌شود. اعتبار ورود به شبکه وایرلس از طرف سرور به سرویس گیرنده اختصاص می‌یابد که به واسطه آن مجوز لازم برای اتصال به شبکه وایرلس را پیدا می‌کند.

۸-۶- WPA2 چگونه عمل می‌کند؟

در اینجا قبل از وارد شدن به بحث اصلی لازم است شمارا با کلیدواژه CCMP آشنا کنیم. CCMP یا پروتکل CCM، پروتکل رمزنگاری است که برای محصولات که بر مبنای استاندارد (IEEE 802.11i که اصلاح شده استاندارد IEEE 802.11 است) در شبکه وایرلس کار می‌کنند طراحی شده است. این پروتکل مکانیزمی سطح بالا در مخفی سازی دیتا در قالب بسته‌های اطلاعاتی دیگر است که برای محرمانگی دیتا طراحی شده است و بر اساس استاندارد AES کار می‌کند. حال به چگونگی کارکرد WPA2 برمی‌گردیم. در روش CCMP، احراز هویت‌های اضافه بر سازمان دیتا (AAD) بر روی هدر MAC و با رمز کردن آن انجام می‌شود و شامل فرآیند رمزنگاری CCM است. این فرآیند کل فریم را از دست کاری احتمالی که بر روی بخش‌های رمز نشده فریم ممکن است رخ دهد، حفظ می‌کند. به عبارتی WPA2 امنیت سطح بالا و احراز هویت‌های قوی خود را علاوه بر حالات موجود، بر روی هدر MAC از یک فریم و با استفاده از پروتکل CCM هم انجام می‌دهد.



شکل ۱۴ - رمزنگاری WPA2

۸-۷- مشکلات امنیتی WPA/WPA2

این پروتکل امنیتی به دلیل استفاده از پ‌سورد ساده همیشه درخطر حملات شکستن پ‌سورد به روش‌های فرهنگ لغت، بروت فورس، ترکیبی و جدول Rainbow قرار دارد.

عدم استفاده از تکنیک پنهان‌سازی روبه‌جلو یا forward secrecy در این پروتکل که تکنیکی که رمزگشایی را سخت می‌کند استفاده نمی‌کنند بدون روش پنهان‌کاری روبه‌جلو یک حمله‌کننده می‌تواند اطلاعات زیادی را به دست آورد و آن‌ها را تنها با یک کلید مخفی رمزگشایی کند. روش forward secrecy به ایمن ماندن به‌وسیله ایجاد کردن یک کلید منحصربه‌فرد برای هر بخش کمک می‌کند به‌عبارت‌دیگر هر بخش به‌وسیله یک کلید سری متفاوت رمزگذاری می‌شود و در صورتی این قسمت انجام می‌پذیرد که مرحله قبلی رمزنگاری end to end صورت گیرد.

Vanhoef, Mathy; Piessens, Frank در تحقیقات خود نشان دادند که استفاده از WPA-TKIP چقدر می‌تواند خطرناک باشد. آن‌ها نشان دادند که چگونه می‌توانند مقدار ۱۱۲ بایت دلخواه را به بسته تزریق کنند و همچنین نشان دادند که چگونه رمزهای دلخواه ارسال شده به یک مشتری را رمزگشایی کنند. آن‌ها افزودند که می‌توان با ربودن اتصال TCP می‌توانند یک کد مخرب جاوا را تزریق نمایند تا وقتی قربانی از وب‌سایت بازدید می‌کند آن را بر روی سیستم او اجرا نمایند.

عدم استفاده MS-Chapv2 از سرور AAA باعث ایجاد مشکل امنیتی در پروتکل WPA2 می‌شود. سرور AAA یک برنامه نرم‌افزاری سرور است که امکان دسترسی کاربران را با منابع کامپیوتری شبکه برقرار می‌کند. این برنامه برای شبکه‌های Enterprise سرویس‌های Authentication, Authorization و Accounting را فراهم می‌آورد. درواقع AAA Server با دسترسی شبکه، سرورهای Gateway، Database ها و جدول‌های اطلاعاتی کاربران در تعامل است. محققان امنیتی در اجلاس امنیتی Defcon ابزاری را منتشر کردند که می‌توانند برای شکستن رمزگذاری هر نشست WPA2 مورد استفاده قرار بگیرند. این نشست‌ها برای احراز هویت از MS-CHAPv2 استفاده می‌کنند. در اجلاس Defcon یکی از محققین امنیتی ابزاری با عنوان ChapCrack را عرضه کرده است. این ابزار می‌تواند از ترافیک شبکه که حاوی MS-CHAPv2 است، تصویربرداری کند و امنیت handshake را به یک کلید واحد DES کاهش دهد. سپس این کلید DES می‌تواند به سایت CloudCracker.com ارائه داده شود و رمزگشایی گردد. خروجی CloudCracker می‌تواند به همراه ChapCrack استفاده شود و کل نشست را رمزگشایی نماید.

آسیب‌پذیری Hole 196 نیز یکی دیگر از آسیب‌پذیری‌های موجود در پروتکل wpa2 است که آسیب‌پذیری مرکزی (GTK) است که در بین همه مشتریان مجاز در شبکه WPA2 به اشتراک گذاشته شده است. در حالت استاندارد، فقط یک AP باید ترافیک داده گروهی را رمزگذاری شده با استفاده از GTK منتقل کند و مشتریان قصد دارند که ترافیک را با استفاده از GTK رمزگشایی کنند. اما با این وجود باز مهاجم می‌تواند بسته‌های جعلی GTK را برای یک سرویس‌گیرنده تزریق کند. با استفاده از این آسیب‌پذیری کاربر مجاز ثالث می‌تواند داده‌های سایر کاربران مجاز را اسنیف و سپس رمزگشایی کند و یا با اسکن کردن دستگاه وایرلس خود آن را آسیب‌پذیر کند.

امکان سوءاستفاده از WPS یا همان QSS در پروتکل WPA نیز باعث نفوذ به دستگاه وایرلس می‌شود. توسط گروه Wi-Fi Alliance در سال ۲۰۰۶ معرفی شد و هدف از آن ارائه قابلیت بود که کاربران خانگی که از تنظیمات و امنیت مودم یا AP آگاهی چندانی نداشتند، بتوانند بدون وارد کردن رمز (PSK) و تنها با استفاده از یک کد ۸ رقمی یا حتی بدون وارد کردن کد، بتوانند به شبکه متصل شوند اما مشکلی اصلی آن این است که نفوذ گر می‌تواند به‌سادگی این کد ۸ رقمی را با استفاده از روش‌های زیر به دست آورد:

- کد پین پیش‌فرض با الگوی ثابت
- بروت فورس آنلاین
- بروت فورس آفلاین (Pixie Dust)
- دسترسی‌های فیزیکی

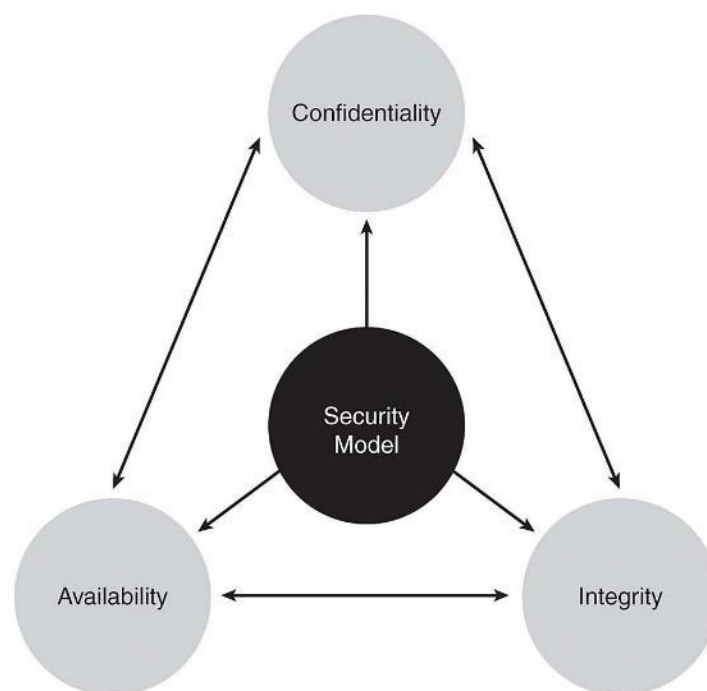
وجود این حملات باعث می‌شود که هکر بتواند به پین کد شما در حداقل ۱ ثانیه و حداکثر ۱۰ ساعت دسترسی پیدا کند.

امکان استفاده از حمله Krack در پروتکل WPA2 نیز یکی دیگر از آسیب‌پذیری‌های این پروتکل است. این حمله توسط Mathy Vanhoef که یک محقق در imec-DistriNet در دانشگاه KU Leuven است، کشف شده است. حمله KRACK توسط بهره‌برداری از روش ۴ طرفه handshake از پروتکل WPA2 که برای ایجاد کلید رمزنگاری ترافیک استفاده می‌شود، کار می‌کند. برای یک حمله موفق KRACK، یک مهاجم نیاز دارد تا قربانی موردنظر را گول بزند تا یک کلید در حال استفاده را مجدداً نصب کند که این امر توسط دست‌کاری و بازپخش

پیام‌های handshake رمزنگاری شده به دست می‌آید. هنگامی که فرد قربانی مجدداً کلید مربوطه را نصب می‌کند، پارامترهای مربوطه مانند تعداد بسته‌های انتقالی افزایشی (به‌عنوان مثال nonce) و تعداد بسته‌های دریافتی (به‌عنوان مثال بازدیدهای مجدد) به مقدار اولیه آن‌ها بازنشانی می‌شوند. اساساً، برای تضمین امنیت، یک کلید فقط باید یک‌بار نصب و استفاده شود. متأسفانه، ما متوجه شدیم که این امر از طریق پروتکل WPA2 تضمین نشده است. با استفاده از دست‌کاری handshake‌های رمزنگاری شده، ما می‌توانیم در عمل از این ضعف سوءاستفاده کنیم.

۹- امنیت

سه اصل اصلی امنیت شبکه رایانه، محرمانه بودن، صداقت و در دسترس بودن است. برای رسیدن به امنیت واقعی، تمام این سه مفاهیم به‌طور خاص موردنیاز است. با استفاده از تمام سه مفاهیم در امنیت شبکه، می‌توان تا درصد بالایی امنیت را تضمین نمود. مهاجمین همیشه در تلاش هستند تا یکی یا بیشتر از این سه اصل امنیتی را به خطر اندازند.



شکل ۱۵- سه اصل امنیت

۹-۱- محرمانگی (Confidentiality)

به معنای آن است که اطلاعات فقط در دسترس کسانی قرار گیرد که به آن نیاز دارند و این‌گونه تعریف شده است. به‌عنوان مثال از دست دادن این خصیصه امنیتی معادل است با بیرون رفتن قسمتی از پرونده محرمانه یک شرکت و امکان دسترسی به آن توسط مطبوعات.

۹-۲- یکپارچگی (Integrity)

بیشتر مفهومی است که به علوم سیستمی بازمی‌گردد و به‌طور خلاصه می‌توان تعریف کرد:

- تغییرات در اطلاعات فقط باید توسط افراد یا پروسه‌های مشخص و مجاز انجام گیرد.
- تغییرات بدون اجازه و بدون دلیل حتی توسط افراد یا پروسه‌های مجاز نباید صورت بگیرد.

-یکپارچگی اطلاعات باید در درون و بیرون سیستم حفظ شود. به این معنی که یک داده مشخص چه در درون سیستم و چه در خارج آن باید یکسان باشد و اگر تغییر کند باید هم‌زمان درون و بیرون سیستم از آن آگاه شوند .

۹-۳- دسترس پذیری (Availability)

این پارامتر ضمانت می‌کند که یک سیستم - مثلاً" اطلاعاتی - همواره باید در دسترس باشد و بتواند کار خود را انجام دهد. بنابراین حتی اگر همه موارد ایمنی مدنظر باشد اما عواملی باعث خوابیدن سیستم شوند-مانند قطع برق از نظر یک سیستم امنیتی این سیستم ایمن نیست. اما جدای از مسائل بالا پارامترهای دیگری نیز هستند که باوجود آنکه از همین اصول گرفته می‌شوند برای خود شخصیت جداگانه‌ای پیدا کرده‌اند. در این میان می‌توان به مفاهیمی نظیر Identification به معنی تقاضای شناسایی به هنگام دسترسی کاربر به سیستم، Authentication به معنی مشخص کردن هویت کاربر، Authorization به معنی مشخص کردن میزان دسترسی کاربر به منابع، Accountability به معنی قابلیت حسابرسی از عملکرد سیستم اشاره کرد.

۹-۴- انواع حملات شبکه‌های وایرلس

شبکه‌های Wireless یا بی‌سیم مدت‌زمانی است که در کشور ما روند رو به رشدی داشته است. در حال حاضر در دانشگاه‌ها، فرودگاه‌ها، مراکز تجاری و اماکنی نظیر آن‌ها دسترسی به اینترنت از طریق شبکه Wireless امکان‌پذیر است. اما نکته‌ای که وجود دارد این است که اگر ایجاد به یک شبکه بی‌سیم برای همه امکان‌پذیر است بنابراین استفاده از آن برای مجرمان و خلاف‌کاران نیز مجاز است! به همین دلیل است که امن سازی این شبکه‌ها و آزمون نفوذ آن بسیار حائز اهمیت است.

۹-۵- حملات کنترل دسترسی

در صورتی که بر روی شبکه‌ی وایرلس اقدامات امنیتی نظیر Mac Filtering یا Access Control صورت گرفته باشد از مجموعه حملات کنترل دسترسی جهت دور زدن اقدامات امنیتی استفاده می‌شود که دارای نوع‌های مختلف می‌باشند که در زیر آن‌ها را معرفی می‌نماییم:

جدول ۵ - انواع حملات کنترل دسترسی

نوع حمله	توضیحات
War Driving	شناسایی شبکه‌های وایرلس با گوش دادن به beacon و ارسال درخواست Probe به سمت آن‌ها انجام می‌شود.
Rogue Access Points	ایجاد یک نقطه اتصال ناامن یا مجازی زیر نظر فایروال که باعث باز شدن یک در پشتی باز در داخل شبکه قابل اعتماد می‌شود.
Ad Hoc Associations	این حمله شامل اتصال مستقیم به یک ایستگاه غیرقانونی برای دور زدن امنیت AP یا حمله به ایستگاه می‌شود. این نوع حملات با نقش مستقیم کارت شبکه وایرلس و یا دانگل (USB Wireless) صورت می‌پذیرد.
MAC Spoofing	این حملات شامل تغییر آدرس مک نفوذ گر به آدرس مک مسیریاب و یا هر سیستم مجاز در داخل شبکه است.
802.1X RADIUS Cracking	این حمله باهدف به دست آوردن رمز رادیوی اقدام به پروت فورس احراز هویت EAP از طریق درخواست دسترسی 802.1X برای نقطه اتصال جعلی مورد استفاده قرار می‌گیرد.

۹-۶- حملات علیه محرمانگی

حملات محرمانه‌ای برای جمع‌آوری اطلاعات خصوصی با رهگیری آن بر روی لینک بی‌سیم تلاش می‌کند. داده‌ها در داخل یک شبکه وایرلس رمزگذاری شده یا به صورت شفاف ارسال می‌شوند. اگر داده‌ها رمزگذاری شوند، این حملات شامل شکستن رمزگذاری و پیدا کردن کلید می‌شود. علاوه بر این شامل حملات دیگر مانند استراق سمع، شکستن پسورد، حملات فیشینگ بر روی نقطه‌ی دسترسی (AP) و حملات مردمیانی نیز است. انواع حملات علیه محرمانگی شامل موارد زیر است:

جدول ۶ - انواع حملات علیه محرمانگی

نوع حمله	توضیحات
Eavesdropping	در ای حملات با گرفتن و رمزگشایی ترافیک انتقال داده شده که به صورت محافظت نشده می‌باشند مهاجم اقدام به گرفتن اطلاعات بالقوه حساس می‌کند.
WEP Key Cracking	این حملات شامل گرفتن اطلاعات برای بازیابی کلید WEP با استفاده از روش‌های غیرفعال یا فعال است.
Evil Twin AP	در این حملات مهاجم یک نقطه دسترسی جعلی را بانام یک نقطه دسترسی مجاز ایجاد می‌کند تا کاربر فریب بخورد و وارد آن شبکه شود.
AP Phishing	این حمله با اجرا کردن یک وب سرور جعلی یا وبسایت بر روی شبکه‌ی Evil Twin اقدام به سرقت اطلاعات، رمزهای عبور و ... می‌کند.
MITM	شکلی از استراق سمع فعال است که در آن حمله‌کننده اتصالات مستقلی را با قربانیان برقرار می‌کند و پیام‌های مابین آن‌ها را بازپخش می‌کند، به گونه‌ای که آن‌ها را معتقد می‌کند که با یکدیگر به طور مستقیم در طول یک اتصال خصوصی، صحبت می‌کنند؛ درحالی که تمام مکالمات توسط حمله‌کننده کنترل می‌شود.

در اینجا به معرفی ابزارهای آزمون نفوذ در شبکه‌های وایرلس بر اساس این سه اصل امنیتی می‌پردازیم.

۹-۷- حملات یکپارچگی

حملات یکپارچگی را می‌توان یک مشخصه دانست که بر اساس آن اطمینان حاصل می‌شود که داده‌ها در هنگام انتقال از نقطه‌ی A به نقطه‌ی B بدون هیچ تغییر یا مشکل انتقال پیدا می‌کند. در شبکه‌های وایرلس 802.11، یک مهاجم می‌تواند با قرار گرفتن در همان سطح فرکانسی به سو استفاده از داده‌های بپردازد. همچنین در این حملات، هکرها فریم‌های جعلی کنترلی یا مدیریتی و یا دیتا را تحت یک شبکه وایرلس ارسال می‌کنند تا دستگاه‌های وایرلس را از مسیر خود منحرف نمایند.

جدول ۷ - انواع حملات علیه یکپارچگی

نوع حمله	توضیحات
802.11 Frame Injection	در این حملات مهاجم به ارسال و یا دست‌کاری فریم‌های جعلی 802.11 می‌پردازد برای این منظور هکر باید به اسنیف داده‌های بین شبکه‌ای بپردازد و اگر داده‌ها مطابق با یک الگوی مشخص شده در فایل‌های پیکربندی باشد، محتوای سفارشی مانند AP داخل شبکه وایرلس تزریق می‌شود و هکر به‌عنوان سرویس‌دهنده در نظر گرفته می‌شود.

در این حملات مهاجم مانند حملات Fram injection به گرفتن پکت ها به گونه ای که از ارسال آنها جلوگیری شود و یک داده ی جدید که حاوی محتوای خاص است را جایگزین می کند و برای سرویس گیرنده ارسال می نماید.	802.11 Data Replay
در این حملات مهاجم اقدام به گرفتن پروتکل احراز هویت قابل تعمیم بین کاربر و دستگاه AP می پردازد تا بتواند بعداً از آنها استفاده کند.	802.1X EAP Replay
در این حملات هکر به گرفتن پیام های RADIUS بین دستگاه AP و سرور احراز هویت می پردازد تا بتواند بعداً از آنها استفاده نماید.	802.1X RADIUS Replay

۸-۹ - حملات علیه احراز هویت

حملات DoS ساده هستند، اما از آنها می توان تنها برای اهداف محدود استفاده کرد. دسترسی به شبکه می تواند مهاجم با مزایای بسیار بیشتری را فراهم کند. از آنجاکه مشخصات اولیه ۸۰۲،۱۱ یک مکانیزم تأیید اعتبار ناقص را تعریف می کند IEEE مکانیسم های احراز هویت جدید را بر اساس ۸۰۲،۱x و EAP معرفی کرده است. در این نوع حملات هکر سعی در شکستن مکانیسم های امنیتی احراز هویت را دارد.

جدول ۸ - حملات علیه احراز هویت

نوع حمله	توضیحات
PSK Cracking	در این حملات مهاجم سعی در به دست آورد کلیدهای WPA/WPA2 PSK در داخل فریم Handshake از طریق حملات فرهنگ لغت یا BruteForce و Hybrid و ... را دارد.
Application Login Theft	در این حملات هکر اقدام به دزدیدن و به دست آوردن کلمه ی عبور از طریق پروتکل های رمزنگاری نشده می کند.
Domain Login Cracking	در آن حملات مهاجم اقدام به گرفتن پسورد حساب های کاربری ویندوز از طریق شکستن پسوردهای هش شده ی پروتکل Netbios با حملات مختلف مانند Bruteforce، حملات فرهنگ لغت و جداول Rainbow و ... می پردازد.
VPN Login Cracking	در آن حملات مهاجم اقدام به گرفتن پسورد PPPT یا IPSec به صورت رمزنگاری شده می کند تا آنها را رمزگشایی کند.
802.1X Identity Theft	این حملات اقدام به، بدست آوردن روش های احراز هویت بدون رمزنگاری در 802.1X می نماید مانند EAP-GTC
802.1X Password Guessing	در ای حمله هکر اقدام به گرفتن داده های رمزنگاری شده از نوع EAP می کند تا بتواند با استفاده از حملات مختلف پسورد رمزنگاری شده را رمزگشایی کند.
802.1X EAP Downgrade	در این حملات هکر اقدام به مجبور کردن یک سرور ۸۰۲،۱x برای ارائه یک نوع تأیید هویت ضعیف با استفاده از جعل بسته های EAP-Response / Nak می کند.

۹-۹ - حملات علیه در دسترس بودن

هدف این گونه حملات ایجاد مانعی در تحویل سرویس وایرلس به کاربر مجاز است که این کار را یا از طریق از دسترس خارج کردن منابع انجام می دهند و یا مانعی در دسترسی به آنها ایجاد می کنند. حملاتی زیادی وجود دارند که در این دسته بندی می گنجند؛ در زیر به برخی از آنها اشاره می کنیم:

جدول ۹ - انواع حملات علیه در دسترسی بودن

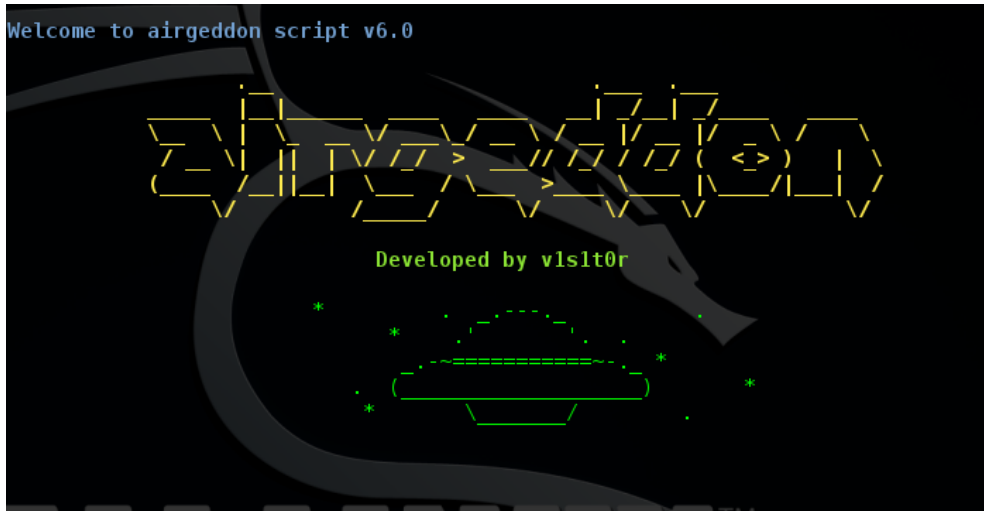
نوع حمله	توضیحات
AP Thief	به صورت فیزیکی اکسس پوینت را از شبکه خارج می کنند.
Queensland DoS	با سوءاستفاده از مکانیزم ارزیابی کانال CSMA/CA، طوری نشان خواهد داد که کانال مورد نظر اشغال است. در این صورت نود دیگری تا زمان آزاد شدن کانال، اطلاعات را ارسال نمی کند. برای این کار کرات شبکه‌ی شما باید از حالت CW Tx پشتیبانی کند.
Beacon Flood ۸۰۲,۱۱	در این حمله مهاجم اقدام به ایجاد هزاران 802.11 beacons می کند تا ایستگاه کاری نتواند AP واقعی را شناسایی کند.
802.11 Associate / Authenticate Flood	در این حملات مهاجم اقدام به ارسال احراز هویت‌ها و ارتباطات جعلی می کند تا جدول ارتباط AP پر شود و دیگر قادر به ایجاد ارتباط با سیستم‌های قانونی و غیر جعلی را نداشته باشد.
802.11 TKIP MIC Exploit	در این حمله مهاجم اقدام به تولید داده‌های نامعتبر TKIP برای عبور از آستانه خطای MIC در AP‌های شبکه می کند تا سرویس‌های شبکه را به تعلیق بی اندازد.
802.11 Deauthenticate Flood	در این حملات مهاجم اقدام به ایجاد سیلی از AP‌ها با پیام EAP-Start می کند تا از این طریق بتواند منابع شبکه را مصرف و یا موجب کرش کردن آن‌ها و یا موجب حذف کاربرهای متصل به آن شود.
802.1X EAP-Failure	در این حمله مهاجم تبادل یک 802.1X EAP-Failure مجاز را زیر نظر گرفته و سپس به Station یک پیام جعلی EAP-Failure ارسال می کند تا منابع داخلی شبکه را مشغول نماید.
802.1X EAP-of-Death	در این حملات مهاجم اقدام به ارسال یک درخواست شناخته شده نادرست برای هویت EAP در 802.1x می کند.
802.1X EAP Length Attacks	در این حمله مهاجم اقدام به ارسال پیام‌های خاص EAP با فیلدهای طولی طولانی می کند که باعث شلوغی زیاد یک سرور AP یا RADIUS می کند و نهایتاً باعث خراب شدن و از کار افتاده شدن آن‌ها می شود.

۱۰- معرفی ابزار

در زیر به معرفی بهترین و جدیدترین ابزارها که توسط متخصصین امنیت جهت آزمون نفوذ به شبکه وایرلس خود مورداستفاده قرار می‌گیرد می‌پردازیم.

Airgeddon

این یک اسکریپت bash چندمنظوره برای سیستم‌های لینوکس برای بررسی شبکه‌های بی‌سیم است.



شکل ۱۶- نمایی از ابزار Airgeddon

GISKismet

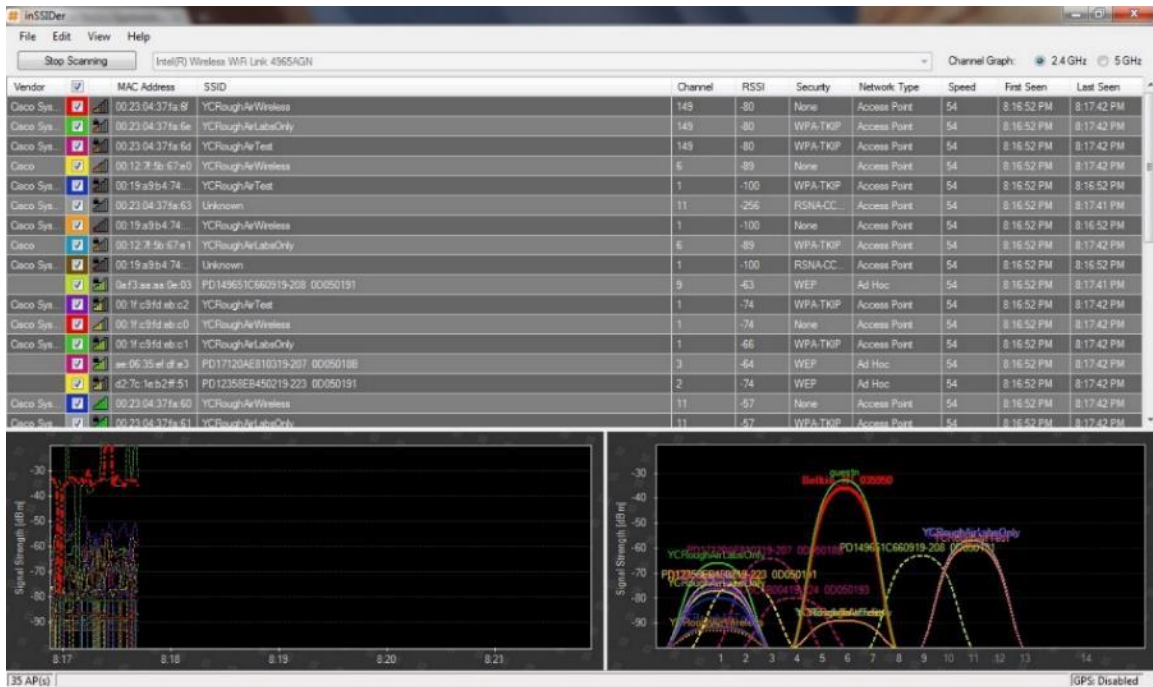
یک ابزار مجازی‌سازی بی‌سیم برای نشان دادن داده‌های جمع‌آوری شده با استفاده از Kismet به یک روش انعطاف‌پذیر و ساده‌تر است.



شکل ۱۷- ابزار GISKismet در لیست ابزارهای تست نفوذ وایرلس در Kali

InSSIDer

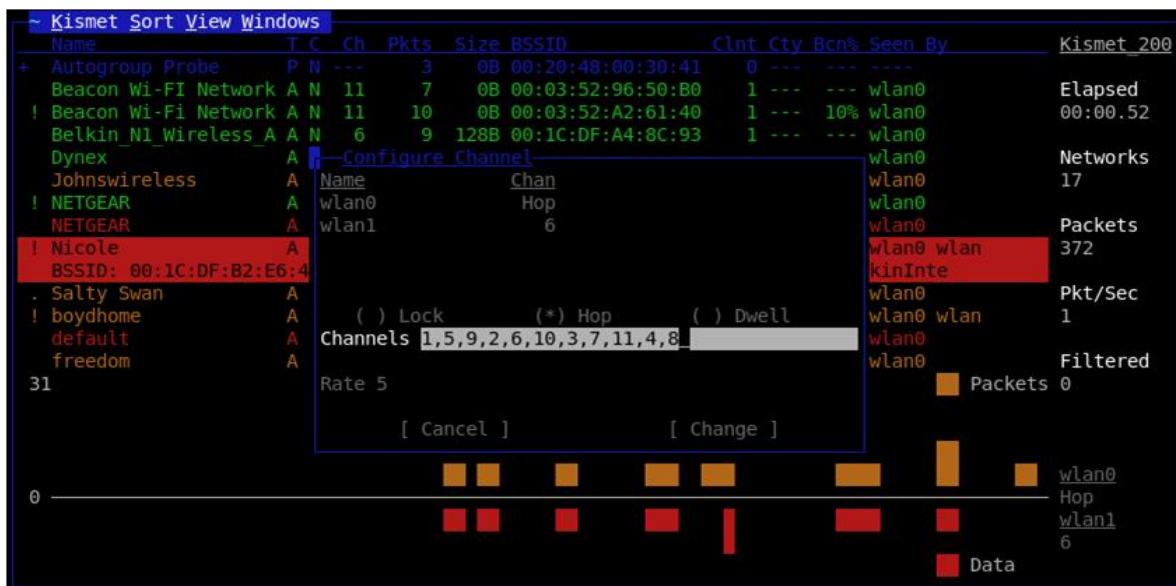
یکی از محبوب ترین ابزارهای نمایش شبکه‌های وایرلس است. همچنین می‌توان از آن به‌عنوان یک برنامه عیب یاب و بهینه سازی نام برد.



شکل ۱۸- نمایی از نرم افزار InSSIDer

Kismet

از این ابزار برای مدیریت شبکه‌های بی سیم و استراق سمع در این شبکه‌ها استفاده می‌شود همچنین می‌توان از آن به‌عنوان یک سیستم تشخیص نفوذ استفاده کرد. این ابزار عمدتاً با شبکه‌های وایرلس IEEE 802.11 کار می‌کند که می‌توان با پلاگین‌های مختلف نیز از آن برای شبکه‌های دیگر استفاده کرد.



شکل ۱۹- نمایی از نرم افزار Kismet

LinSSID

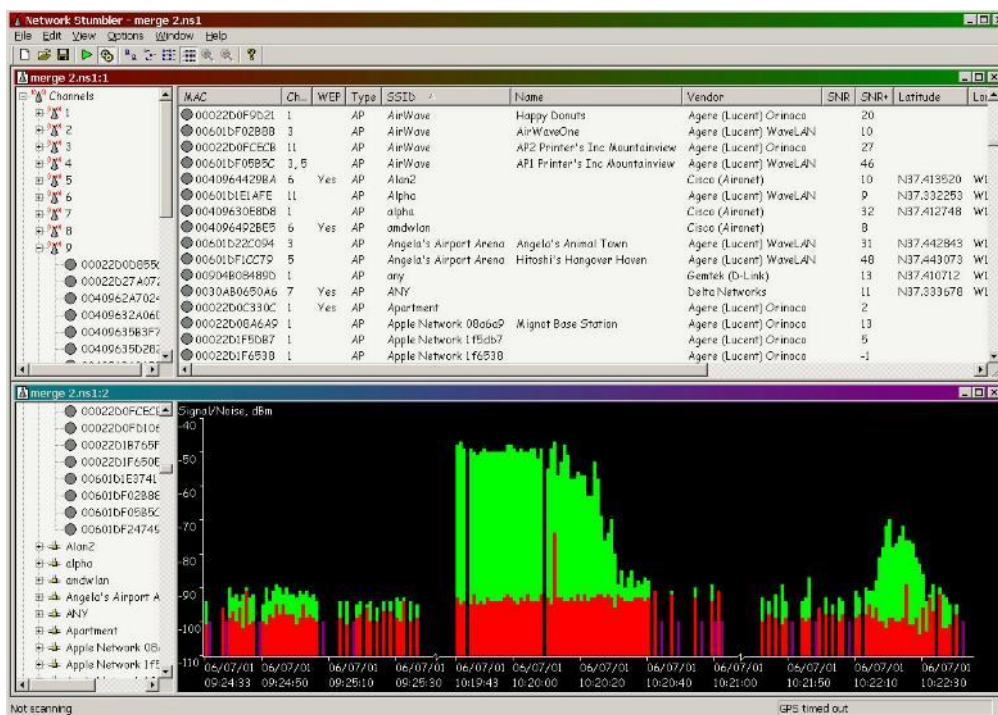
یک برنامه جهت اسکن بی‌سیم برای لینوکس با رابط کاربری گرافیکی خوب است که مشخصاتی کلی را در مورد یک شبکه وایرلس نشان می‌دهد.



شکل ۲۰- نمایی از نرم افزار LinSSID

NetStumbler

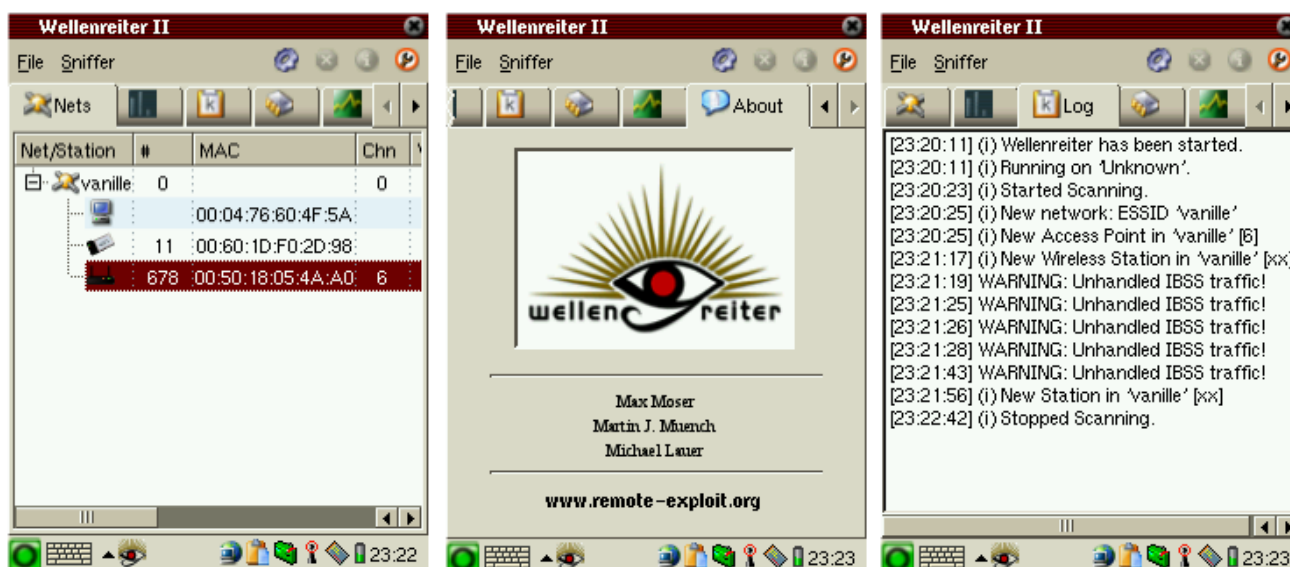
یک ابزار برای ویندوز است که تشخیص شبکه‌های بی‌سیم را با استفاده از استاندارد های 8۰۲,۱۱b, 8۰۲,۱۱a و 8۰۲,۱۱g تسهیل می‌کند.



شکل ۲۱- نمایی از ابزار NetStumbler

Wellenreiter

یک ابزار کشف و حسابرسی شبکه بی‌سیم است.



شکل ۲۲- نمایی از ابزار Wellenreiter

whoishere.py

این نرم افزار قابلیت تشخیص کاربران متصل به وایرلس با ارسال درخواست prob برای آن‌ها را دارد.

```

seclist@server:~/network/whoishere.py$ ls
README.md  screenshots  whoisherell.conf  whoishere.py
seclist@server:~/network/whoishere.py$ sudo python2 whoishere.py

W|H|O|I|S|H|E|R|E

WIFI Client Detection 0.2

Author: Pedro Joaquin @_hkm (pjoaquin@websec.mx)
To kill this script hit CTRL-C

[+] No configuration file found.
[+] Example configuration file created: [whoishere.conf]
[+] Modify configuration file to add monitor interface and list of names and MACs.
[+] Then run 'python whoishere.py'
    
```

شکل ۲۳- نمایی از ابزار CLI با نام whoishere.py نوشته شده در پایتون

WifiChannelMonitor

این برنامه قابلیت ضبط کردن و اسنایف ترافیک، در داخل کانالی که توسط کاربر در نرم افزار انتخاب کرده را دارد. و با استفاده از درایور مونیترینگ شبکه در مایکروسافت می تواند در حالت monitoring mode کاربران متصل به شبکه را می تواند پیدا کند.

SSID	MAC Address	Company	PHY Type	Frequency	Channel	RSSI	Security	Cipher	Beacons	Probe Re...	Data Bytes	Rx
M...	BC-F6-85-0...	D-Link International	802.11n	2437	6	-86	WPA2-PSK	CCMP	2,966	3,063	448	0
il...	9C-D6-43-...	D-Link International	802.11n	2437	6	-86	WPA2-PSK	CCMP	6,093	2,435	530	0
s...	BC-F6-85-0...	D-Link International	802.11n	2437	6	-88	WPA2-PSK	CCMP	5,167	1,053	19,335	0
n...	9C-D6-43-...	D-Link International	802.11n	2437	6	-79	WEP	WEP	5,745	995	3,005	0
m...	C8-BE-19-1...	D-Link International	802.11n	2437	6	-87	WPA2-PSK	CCMP	4,795	867	52,001	1,
S...	84-C9-B2-B...	D-Link International	802.11n	2437	6	-84	WEP	WEP	5,901	589	64,785	0
D...	2E-D0-5A-...	D-Link International	802.11n	2437	6	-76	WPA2-PSK	CCMP	208	232	0	0
B...	34-08-04-0...	D-Link Corporation	802.11n	2437	6	-87	None	None	697	208	93,105	67
M...	C4-3D-C7-...	NETGEAR	802.11n	2437	6	-92	WPA2-PSK	CCMP	4,196	202	8,673	1,
R...	00-1F-1F-0...	Edimax Technology C...	802.11g	2437	6	-84	WEP	WEP	1,229	164	26,642	2,
B...	30-46-9A-2...	NETGEAR	802.11g	2437	6	-54	None	None	5,110	163	2,216	0
B...	62-BE-19-1...	NETGEAR	802.11n	2437	6	-86	None	None	4,116	142	0	0
t...	54-E6-FC-...	TP-LINK TECHNOLOG...	802.11n	2437	4	-78	WPA-PSK ...	TKIP+CCMP	1,623	125	0	0

MAC Address	Company	RSSI	SSID List	Sent Data Bytes	Received ...	Retransmitted ...	Retransmitted ...	Client Type	Device Name
60-6B-BD-5...	Samsung Electronics Co...	-93		4,104	1,492	76	1,160	Wifi Client	
90-B2-1F-4...	Apple	-85		496	1,253	0	251	Wifi Client	
C4-3D-C7-...	NETGEAR	-92		3,467	1,102	1,527	0	Router	
00-1C-85-0...	Eunicorn	-83		606	664	0	58	Wifi Client	
8C-29-37-1...	Apple			0	58	0	58	Unknown	

40 APs, 5 Clients
NirSoft Freeware. <http://www.nirsoft.net>

شکل ۲۴ - نمایی از ابزار WifiChannelMonitor

WifiInfoView

شبکه‌های بی‌سیم را در منطقه شما اسکن و اطلاعات گسترده ای را در مورد آن‌ها نمایش می‌دهد.

SSID	MAC Address	PHY Type	RSSI	Signal Quality	Frequency	Channel	Information Size	Elements Count	Company
Wifi_Gaal	00-13-7F-E6-0E-3E	802.11g	-91	15	2.467	12	83	8	SMC Networks, Inc.
WIFIBEAT	00-00-00-09-84-B0	802.11g	-85	25	2.447	8	56	8	XAVi Technologies Corp.
WLAN471	00-22-3B-44-71-D9	802.11g	-90	16	2.427	4	224	9	SMC Networks Inc.
WLAN7D	00-13-7F-E7-DA-86	802.11g	-90	16	2.412	1	82	8	SMC Networks, Inc.
WLAN_3E	0C-0C-A3-21-3E-...	802.11n	-88	20	2.437	6	231	19	Amper
WLAN_43	00-1B-15-D5-43-1E	802.11g	-86	23	2.412	1	79	8	TECOM Co., Ltd.
WLAN_5A	AA-52-0F-EA-5A-FE	802.11n	-88	20	2.437	6	280	12	ADB Broadband Italia
WLAN_76	64-6B-0C-4A-76-40	802.11g	-90	16	2.422	3	209	10	COMTREND
WLAN_AF	64-6B-0C-BA-8A-14	802.11g	-90	16	2.457	10	64	7	TP-LINK TECHNOLOGIE...

Element ID: 0 (SSID)
57 69 66 69 5F 47 61 Wifi_Gaal

Element ID: 1 (Supported Rates)
82 84 8B 96 0C 12 18 24

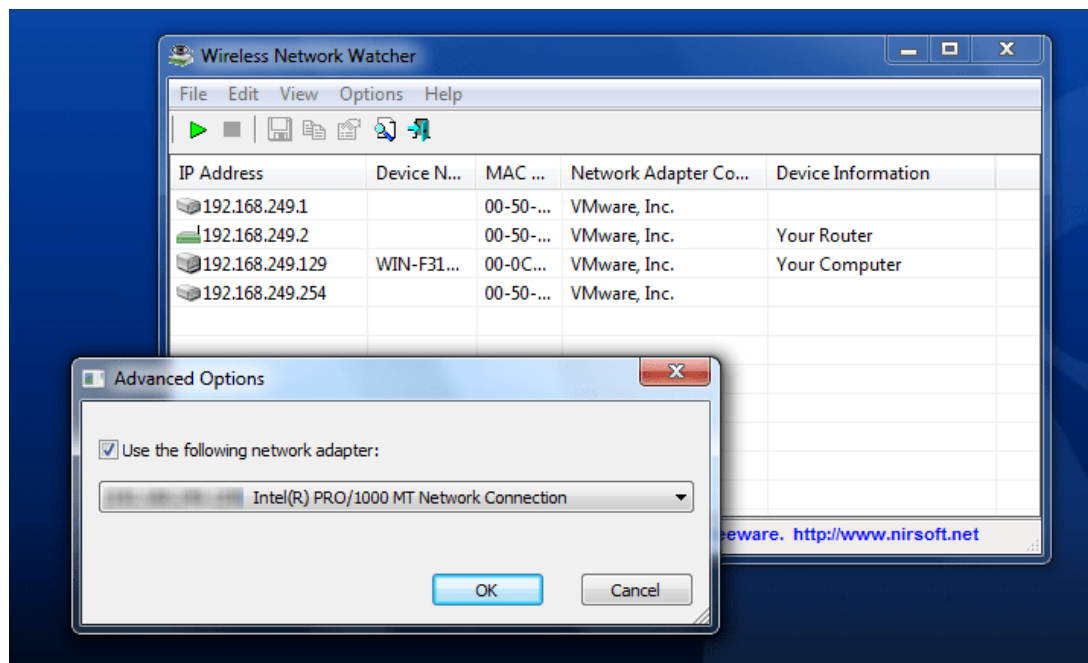
Element ID: 3 (DS Parameter Set)
0C

67 item(s), 1 Selected
NirSoft Freeware. <http://www.nirsoft.net>

شکل ۲۵ - نمایی از ابزار WifiInfoView

Wireless Network Watcher

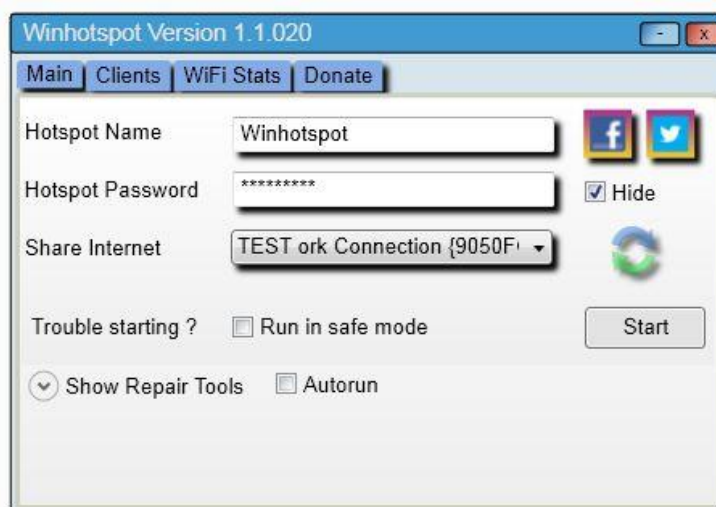
یک ابزار کوچک است که شبکه بی‌سیم شما را اسکن می‌کند و فهرستی از تمام رایانه‌ها و دستگاه‌هایی که در حال حاضر به شبکه شما متصل هستند نمایش می‌دهد.



شکل ۲۶ - نمایشی از ابزار Wireless Network Watcher

Winhotspot

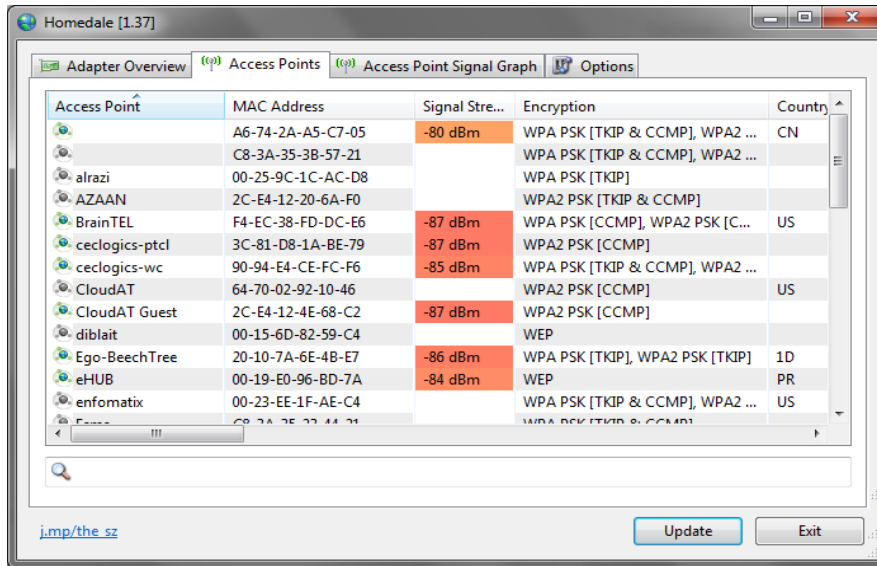
این برنامه در واقع یک برنامه مستقل است که به شما امکان می‌دهد به آسانی یک نقطه‌ی اتصال را برای اتصال اینترنت خود با استفاده از آداپتور بی‌سیم خود ایجاد کنید. با این حال آن را نیز می‌توانید به‌عنوان یک اسکریپت شبکه‌های بی‌سیم همراه با آمار دسترسی نشان داد حتی شبکه‌های وایرلس مخفی شده را نیز می‌توان اسکن کرد.



شکل ۲۷ - نمایشی از ابزار Winhotspot

Homedal

Homedal (نظرسنجی کامل ما را بخوانید) یکی دیگر از ابزار مانیتورینگ قابل حمل و بی‌سیم است که قادر به نشان دادن شبکه‌های بی‌سیم پنهان است. این برنامه دارای چهار قسمت مختلف است. که نمای کلی آ‌پاتور بی‌سیم، نقاط دسترسی، نمودار سیگنال و گزینه‌ها را نشان می‌دهد. در برگه Access Points شما می‌توانید تمام شبکه‌های تشخیص داده‌شده را مشاهده کنید با سطوح قدرت سیگنال به‌صورت خودکار هر چند ثانیه به‌روزرسانی می‌شود.



شکل ۲۸ - نمای از ابزار Homedal

NetSurveyor

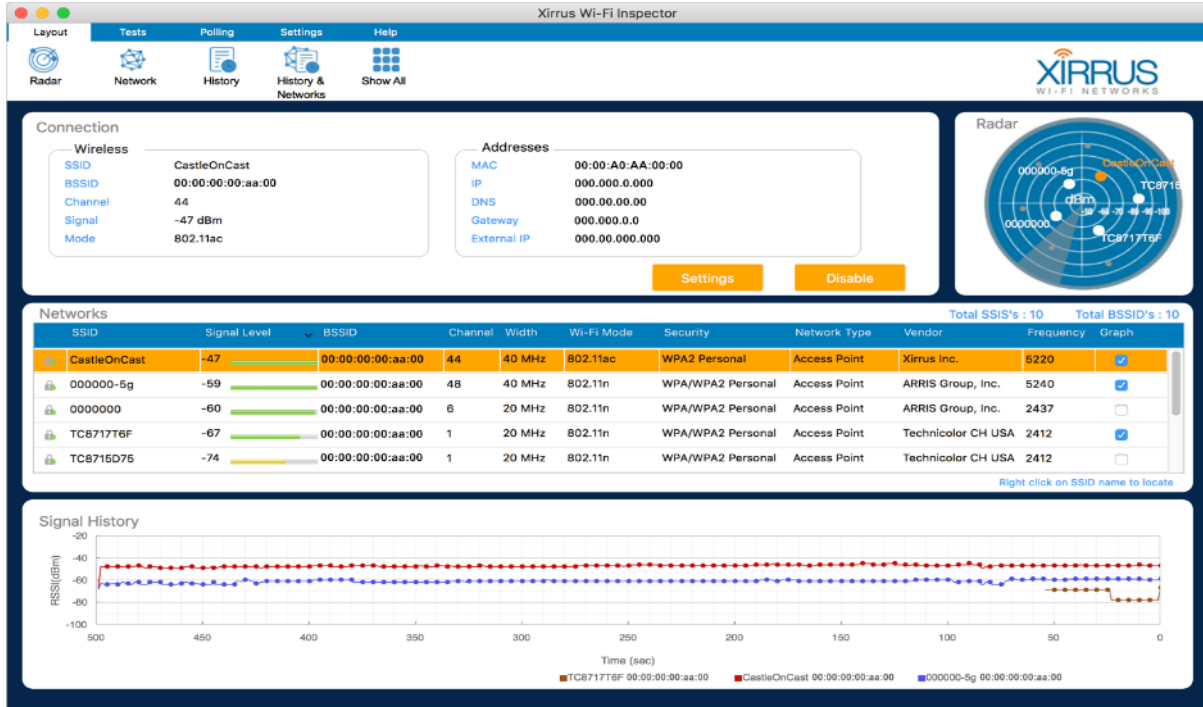
NetSurveyor توسط Nuts About Nets به نظر می‌رسد ابزار حرفه‌ای تر از آن است که با ورود به سیستم برای ضبط و پخش داده‌ها می‌آید. این برنامه قابلیت ارائه‌ی یک خروجی که شامل مشخصات و اطلاعات در مورد شبکه‌ی وایرلس است را دارد مانند: شبکه‌های کشف‌شده، کیفیت وایرلس و ... را با گراف رابطه کاربری قدرتمند، نشان می‌دهد.



شکل ۲۹ - نمای از ابزار NetSurveyor

Xirrus Wi-Fi Inspector

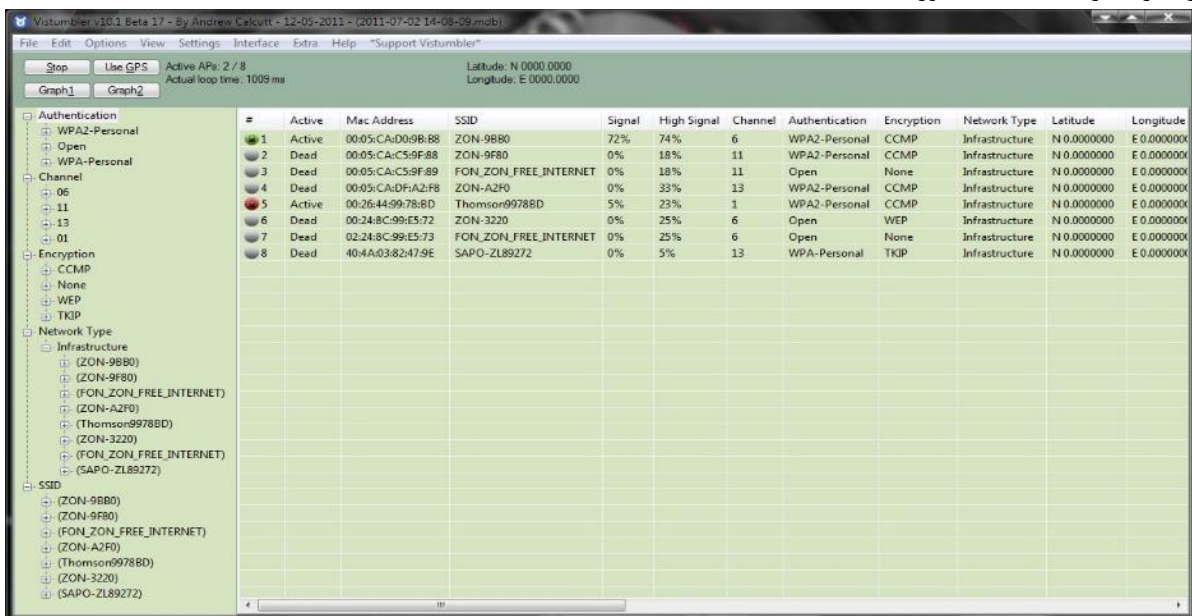
این برنامه یک رابط کاربری مدرن دارد که امکانات فراوانی مانند رادار، اطلاعات ارتباطی، شبکه‌های موجود و تاریخ سیگنال و ... را به کاربر ارائه می‌کند همچنین می‌توان به‌عنوان یک ابزار برای رفع مشکلات شبکه از آن بهره برد.



شکل ۳۰ - نمایشی از ابزار Xirrus Wi-Fi Inspector

Vistumbler

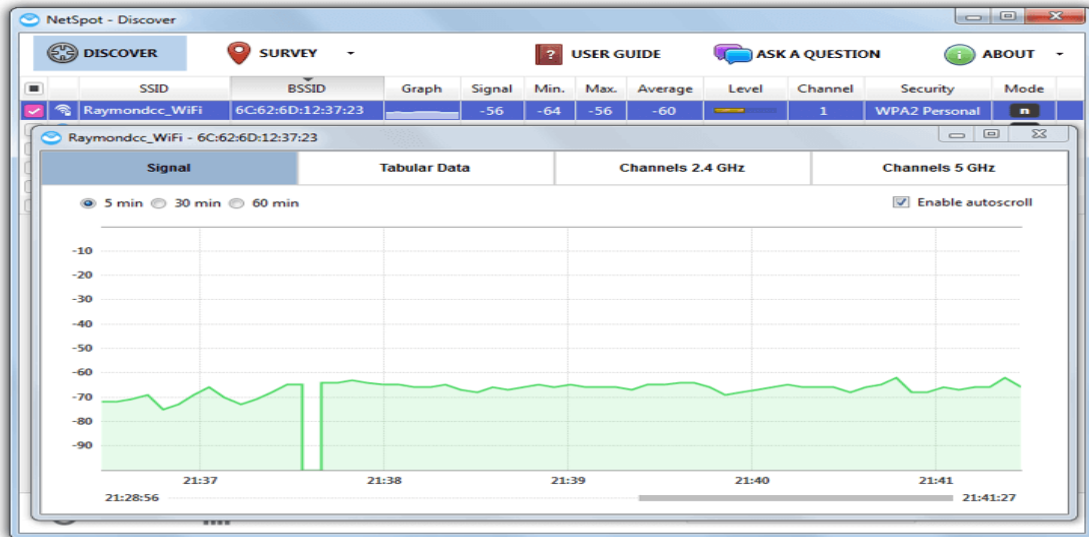
این برنامه یک اسکریپت وایرلس‌های اطراف است که به جای برنامه NetStumbler شد که می‌تواند اطلاعات مفیدی در رابطه با شبکه‌های وایرلس اطراف برای ما به دست آورد.



شکل ۳۱ - نمایشی از ابزار Vistumbler

NetSpot

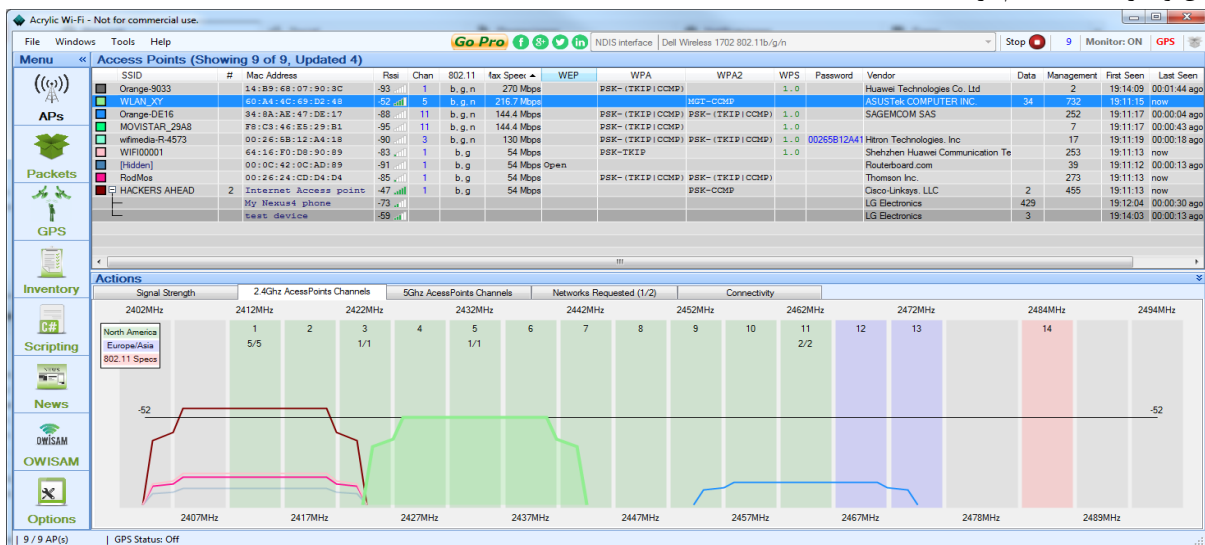
NetSpot یک سیستم تجزیه و تحلیل سیگنال و ابزار عیب یابی شبکه بی سیم رایگان برای هر دو کامپیوتر مکینتاش و ویندوز است. علاوه بر یک بخش کشف و نظارت وایفای استاندارد، همچنین دارای ویژگی بررسی سایت است که اجازه می دهد تا قدرت سیگنال شبکه‌ی مربوط، بر روی نقشه ساختمان یا منطقه محلی شما طراحی شود.



شکل ۳۲- نمایی از ابزار NetSpot

Acrylic WiFi

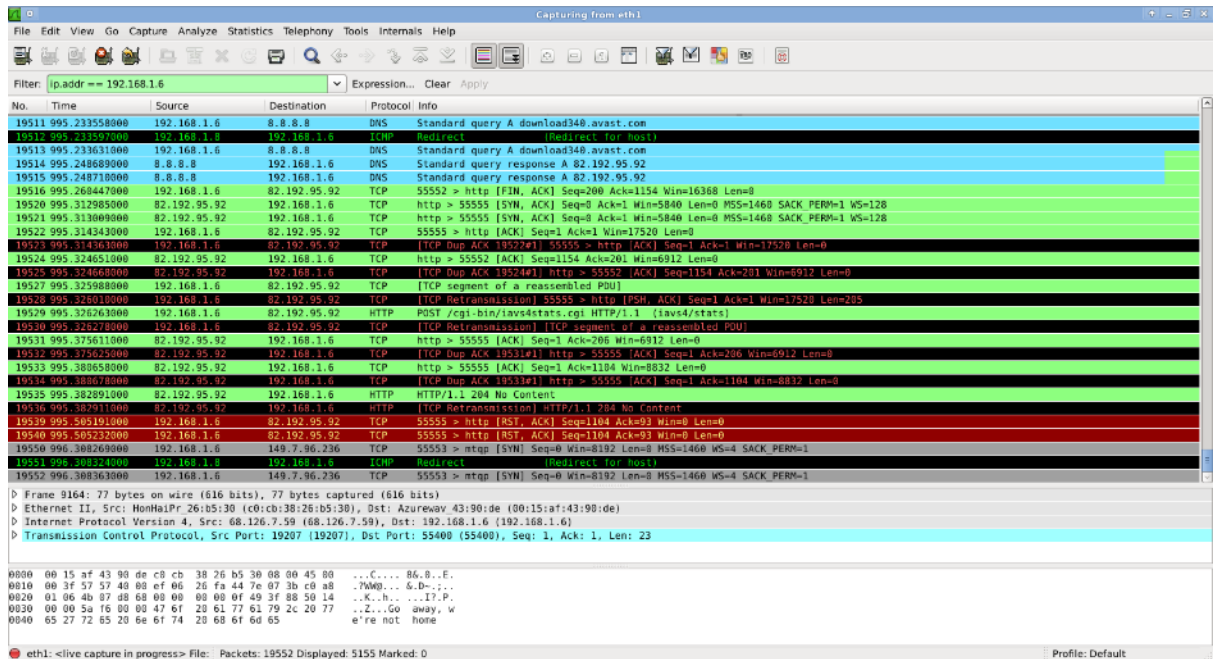
Acrylic WiFi یکی از بهترین نرم افزار های تجزیه و تحلیل wifi، برای شناسایی نقاط دسترسی و کانال های wifi و شناسایی و رفع مشکلات آن بر روی شبکه‌های بی سیم ۸۰۲.۱۱ a/b/g/n/ac است. این نرم افزار امکان کنترل سطح عملکرد شبکه، اطلاع و کنترل از افراد متصل به شبکه، مشخص کردن سرعت انتقال اطلاعات و داده‌ها و سازماندهی شبکه‌های wifi را به کاربران و تحلیلگران شبکه‌های بی سیم می دهد. از دیگر امکانات این نرم افزار می توان به دسترسی به اطلاعات و جزئیات شبکه بی سیم شامل شبکه‌های مخفی و ساخت ویژگی های منحصر به فرد مانند حالت نظارتی برای ضبط و تجزیه و تحلیل ترافیک تمامی دستگاه های وایرلس، مشاهده دستگاه ها، ابزارهای در دسترس و سرعت wifi، نام برد.



شکل ۳۳ - نمایی از ابزار Acrylic WiFi

Wireshark

Wireshark یک ابزار تجزیه و تحلیل پیشرفته پروتکل شبکه است که برای رهگیری ترافیک، نظارت بر ارسال/دریافت بسته‌های داده، بررسی مسائل مربوط به شبکه و فعالیت های مشکوک، آمارگیری و ... می‌تواند مورد استفاده قرار گیرد. وایرشارک در سرتاسر جهان به‌عنوان نرم‌افزاری پیشرو برای آنالیز پروتکل‌های شبکه مورد استفاده قرار می‌گیرد و امکانی را فراهم می‌کند تا تمام آنچه در شبکه رخ می‌دهد را به‌صورت مو به مو (در سطح ماکروسکوپی و با جزئیات) مشاهده کنید. به‌طور کلی Wireshark برای عیب‌یابی شبکه، تجزیه و تحلیل نرم‌افزارها و توسعه پروتکل‌های ارتباطی و آموزش استفاده می‌شود و به‌عنوان یک استاندارد واحد در بسیاری از صنایع و موسسات مورد استفاده قرار می‌گیرد.

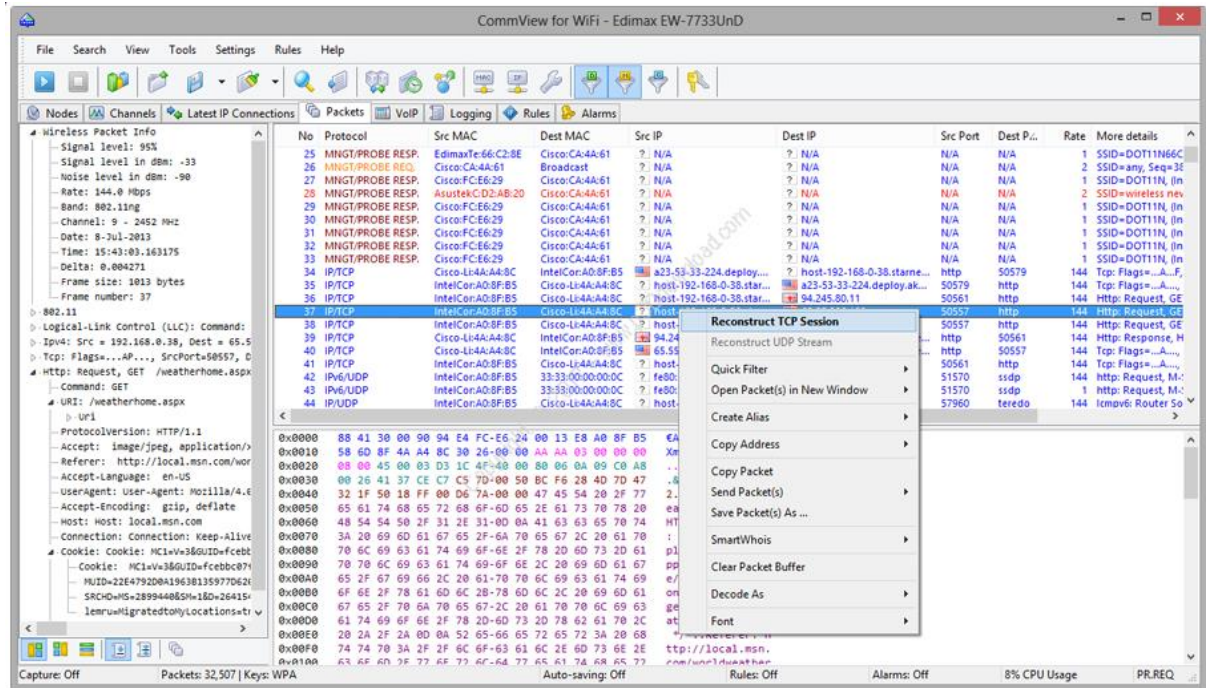


شکل ۳۴ - نمایشی از ابزار Wireshark

CommView for WiFi

ابزاری قدرتمند برای کنترل شبکه‌های وایرلس و آنالیزوری برای شبکه‌های ۸۰۲.۱۱ a/b/g/n/ac است. این نرم‌افزار قدرتمند ترکیبی از ویژگی‌های منحصر به فرد به همراه یک رابط کاربری مناسب است. CommView for WiFi تمام بسته‌های داده‌ای موجود در فضا را جهت به دست آوردن و نمایش اطلاعات مهمی چون فهرستی از نقاط دسترسی و ایستگاه‌ها، آمار هر گره و هر کانال، قدرت سیگنال، فهرستی از بسته‌ها و اتصالات شبکه، نمودارهای توزیع پروتکل و ... را ضبط می‌کند. با اطلاعات به دست آمده به کمک این نرم‌افزار می‌توانید بسته‌های داده را مشاهده و بررسی کرده، مشکلات شبکه را دقیقاً مشخص و اشکالات سخت‌افزاری و نرم‌افزاری را برطرف کنید. CommView for WiFi شامل یک ماژول VoIP برای تجزیه و تحلیل دقیق، ضبط و پخش ارتباطات صوتی SIP و H.323 است. بسته‌های داده‌ای می‌توانند با استفاده از WEP تعریف شده توسط کاربر یا کلیدهای WPA/WPA2-PSK رمزگذاری شده و یا در سطح پایین‌ترین لایه رمزگشایی شوند.

این نرم‌افزار با پشتیبانی از بیش از ۱۰۰ پروتکل امکان مشاهده تمام جزئیات بسته‌های ضبط شده را به آسانی به‌صورت یک ساختار درختی فراهم کرده تا بتوان لایه‌های پروتکل و عناوین بسته‌ها را مشاهده کرد.



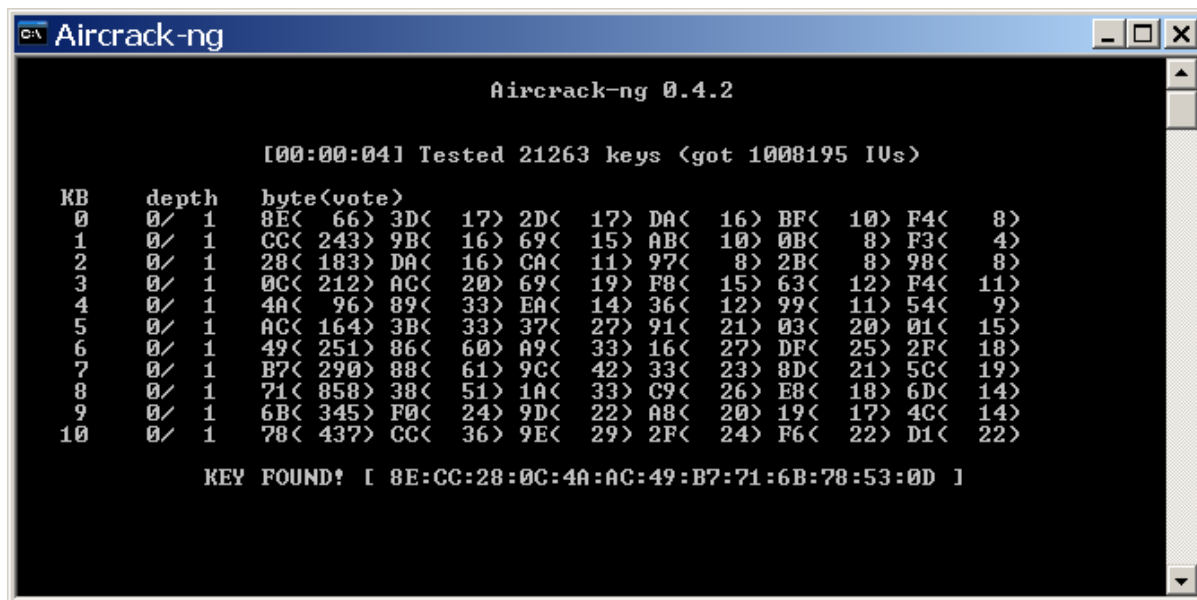
شکل ۳۵ - نمایش از ابزار CommView for WiFi

قابلیت های کلیدی نرم افزار CommView for WiFi:

- اسکن فضا برای کشف ایستگاه‌های WiFi و نقاط دسترسی
- ضبط ترافیک 802.11n، 802.11g، 802.11b، 802.11a، و 802.11ac WLAN
- مشخص کردن کلیدهای WEP یا WPA برای رمزگشایی بسته‌های رمزگذاری شده
- مشاهده آمار دقیق در هر گره و هر کانال
- مشاهده آمار جزئیات اتصالات IP: آدرس های IP، پورت ها، سشن ها و ...
- بازبینی بخش های TCP
- آلامر هایی برای هشدار هنگام وقوع رویدادهای مهم مانند شناسایی بسته‌های مشکوک، استفاده زیاد از پهنای باند، آدرس های ناشناخته و ...
- مشاهده نمودار های "pie" پروتکل
- کنترل پهنای باند استفاده شده
- بررسی لحظه ای بسته‌های داده رمزگشایی شده
- جستجوی رشته‌ها یا داده‌های هگزا در محتوای بسته ها
- بارگذاری و مشاهده فایل‌های ضبط شده در حالت آفلاین
- وارد کردن یا استخراج بسته ها در قالب های Sniffer®، EtherPeek™، AiroPeek™، Observer®، NetMon، Wireshark / Tcpdump
- و استخراج بسته‌های حاوی داده‌های هگزا یا فرمت های متنی
- استخراج هر آدرس IP در SmartWhois برای جستجو سریع و آسان آی پی
- ضبط داده‌ها از چندین کانال با استفاده از چند آداپتور USB به صورت هم‌زمان
- ضبط بسته‌های A-MSDU و A-MPDU
- شبیه سازی نقاط دسترسی
- و ...

Aircrack-ng

ابزار aircrack-ng یک مجموعه کامل از ابزارها برای ارزیابی امنیت شبکه WiFi است. این ابزار از استانداردهای مختلف مانند 802.11b, 802.11g, پشتیبانی می‌کند و برای ورژن‌های مختلف آن برای تمامی پلتفرم‌های linux, FreeBSD, OS X, OpenBSD و windows وجود دارد.



```

Aircrack-ng 0.4.2

[00:00:04] Tested 21263 keys (got 1008195 IVs)

KB  depth  byte(vote)
0   0/ 1     8E< 66> 3D< 17> 2D< 17> DA< 16> BF< 10> F4< 8>
1   0/ 1     CC< 243> 9B< 16> 69< 15> AB< 10> 0B< 8> F3< 4>
2   0/ 1     28< 183> DA< 16> CA< 11> 97< 8> 2B< 8> 98< 8>
3   0/ 1     0C< 212> AC< 20> 69< 19> F8< 15> 63< 12> F4< 11>
4   0/ 1     4A< 96> 89< 33> EA< 14> 36< 12> 99< 11> 54< 9>
5   0/ 1     AC< 164> 3B< 33> 37< 27> 91< 21> 03< 20> 01< 15>
6   0/ 1     49< 251> 86< 60> A9< 33> 16< 27> DF< 25> 2F< 18>
7   0/ 1     B7< 290> 88< 61> 9C< 42> 33< 23> 8D< 21> 5C< 19>
8   0/ 1     71< 858> 38< 51> 1A< 33> C9< 26> E8< 18> 6D< 14>
9   0/ 1     6B< 345> F0< 24> 9D< 22> A8< 20> 19< 17> 4C< 14>
10  0/ 1     78< 437> CC< 36> 9E< 29> 2F< 24> F6< 22> D1< 22>

KEY FOUND! [ 8E:CC:28:0C:4A:AC:49:B7:71:6B:78:53:0D ]
    
```

شکل ۳۶ - تمایی کلی از ابزار Aircrack-ng

ابزار aircrack-ng تنها توانایی انجام آزمون نفوذ بر روی شبکه را انجام می‌دهد بلکه می‌تواند شبکه را مورد حمله قرار دهد به هرکس اجازه می‌دهد که به پسورد دسترسی پیدا کند.

از ویژگی‌های این برنامه می‌توان به موارد زیر اشاره نمود:

نظارت: ثبت بسته و صدور داده‌ها به فایل‌های متنی برای پردازش بیشتر توسط ابزارهای ثالث.

حمله: حمله پاسخ، ایجاد نقاط دسترسی جعلی از طریق تزریق بسته.

آزمون: چک کردن کارت‌های WiFi و قابلیت‌های درایور (ثبت و تزریق)

اری برای کرک رمزهای عبور WEP و WPA و WPA2

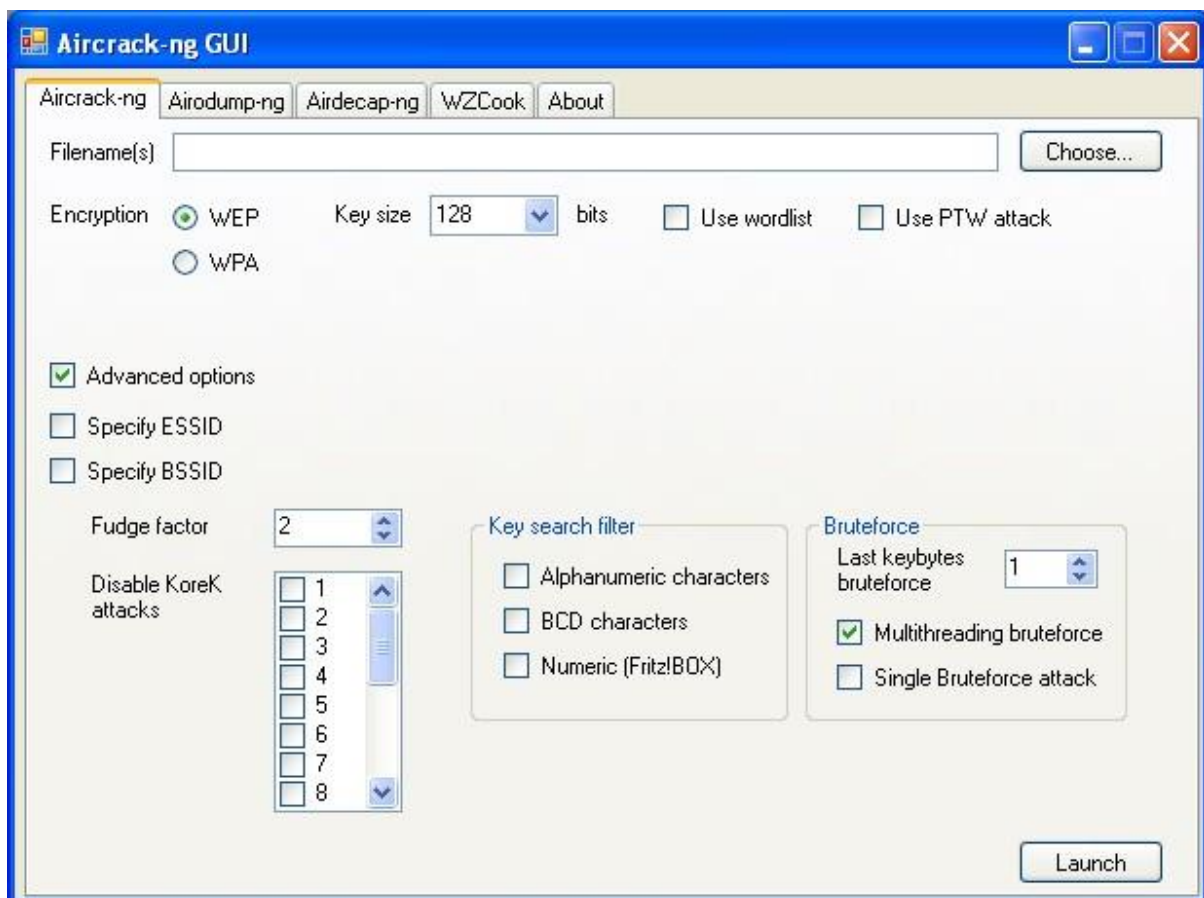
مجموعه نرم‌افزاری aircrack شامل نرم‌افزارهای زیر است:

جدول ۱۰ - فهرستی از مجموعه ابزارهای AirCrack-NG

نام ابزار	توضیحات
aircrack-ng	برنامه‌ای جهت شکستن پسوردهای WEP 802.11 و WPA/WPA2-PSK
airdecap-ng	جهت رمزگشایی بسته‌های دریافت شده (Capture File) از پروتکل‌های WEP, WPA/WPA2 استفاده می‌شود.
airmon-ng	ابزاری برای فعال‌سازی monitor-mode در کارت شبکه‌های وایرلس.
aireplay-ng	ابزاری برای تزریق بسته یا بستک به درون شبکه‌های وایرلس.
Airodump	Airodump-ng برای گرفتن بسته فریم‌های خام 802.11 استفاده می‌شود و مخصوصاً برای جمع‌آوری (Vectorisation Vector) WEP IV به منظور استفاده از آن‌ها در aircrack-ng است.
airtun-ng	یک برنامه جهت ساهتن رابط تونل مجازی است.

packetforge-ng	ابزاری برای ساخت انواع مختلفی از بسته‌های رمزگذاری شده که از آن می‌توان برای تزریق استفاده کرد.
airbase-ng	ابزاری برای ساخت اکسس پوینت های جعلی و تقلبی که به ما امکان استفاده از حملات MITM را می‌دهد.
airdecloak-ng	ابزاری برای حذف فایل WEP Cloak از فایل‌های pcap.
airolib-ng	برای ذخیره و مدیریت لیست های essid و password ها و کلیدهای PMK و از آن‌ها در شکستن پسوردهای WPA / WPA2 در AirCrack-ng استفاده می‌کند.
airserv-ng	کارت بی‌سیم سرور TCP/IP است که اجازه‌ی استفاده چند برنامه را به‌صورت هم‌زمان به این کارت را می‌دهد.
esside-ng	این ابزار امکان برقراری ارتباط به نقطه دسترسی که با الگوریتم رمزگذاری WEP پیکربندی شده است را بدون دانستن کلید می‌دهد.
tkiptun-ng	ابزاری برای انجام حملات WPA/TKIP با استفاده از تزریق چند فریم به WPA TKIP شبکه با QoS
wessid-ng	این ابزار شامل تعدادی از روش‌های یکپارچه برای به دست آوردن کلید WEP در کمترین زمان ممکن است.

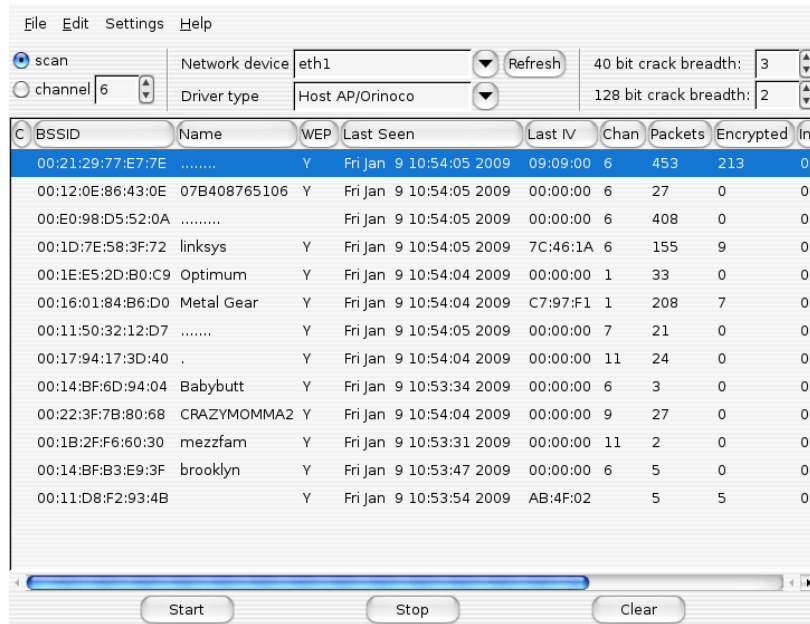
لازم به ذکر است که این ابزار دارای یک ورژن GUI نیز است که توسط خود توسعه دهنده ی این برنامه نوشته شده است.



شکل ۳۷ - نمایی از نسخه گرافیکی Aircrack-ng

AirSnort

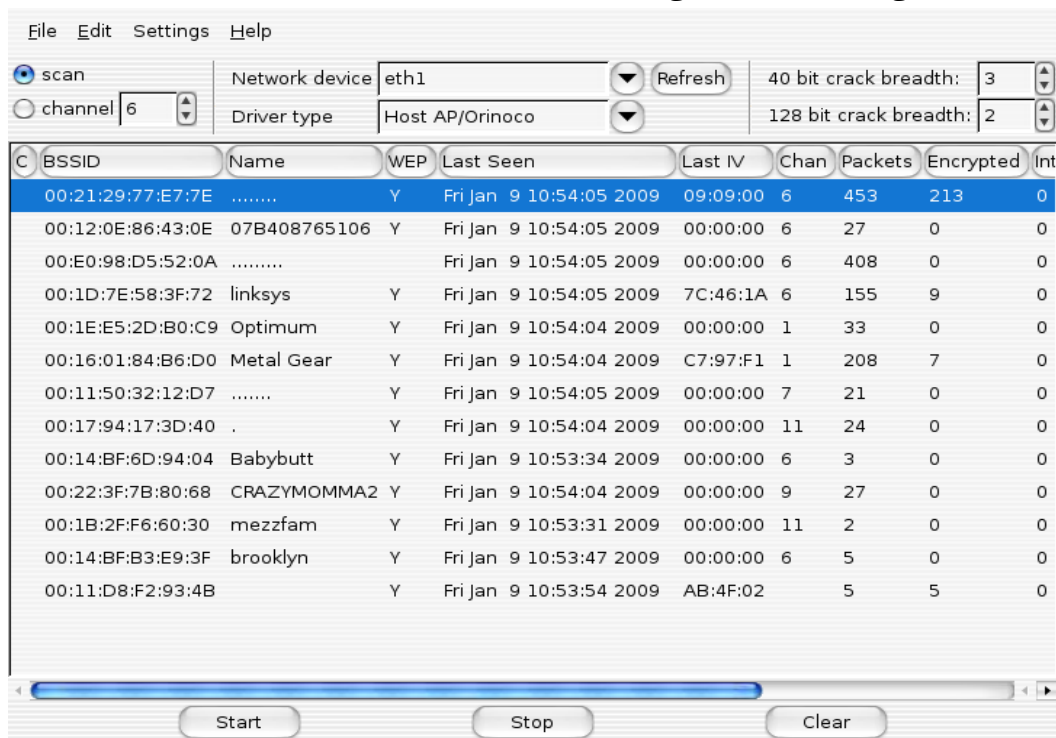
یک برنامه‌ی برای شبکه‌های بی‌سیم که توانایی شکستن پسورد کلیدهای WEP را در شبکه‌های استاندارد 802.11b را دارد.



شکل ۳۸ - نمایشی از ابزار AirSnort

Asleep

نقص جدی در شبکه‌های اختصاصی سیسکو LEAP نشان می‌دهد. پروتکل LEAP در سیستم‌های بی‌سیم سیسکو از MS-CHAPv2 برای مبادله احراز هویت استفاده می‌کند و این امر باعث می‌شود که به حملات فرهنگ لغت آفلاین شکسته شود.



شکل ۳۹ - نمایشی از ابزار Asleep

Auto Reaver

یک اسکریپت در لینوکس که توسط bash نوشته شده است که به ما امکان حمله به چند نقطه‌ی اتصال را که توسط ابزار Reaver انجام می‌شود، با استفاده لیست BSSID در داخل یک فایل متنی را فراهم می‌کند. ابزار Reaver توانایی آزمودن کلیدهای WPS را با استفاده از حملات Brute-force دارد و همچنین امکان استخراج پسورد وایرلس‌های محافظت شده توسط رمزنگاری WPA را دارد.

```
[+] Switching wlan0 to channel 6
[+] Waiting for beacon from 70:54:D2:D5:98:E5
[+] Associated with 70:54:D2:D5:98:E5 (ESSID: 744edc)
[+] Trying pin 12345670
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 3 seconds
[+] WPS PIN: '12345670'
[+] WPA PSK: 
[+] AP SSID:
```

شکل ۴۰ - نمایشی از ابزار Auto Reaver

Auto_EAP

این ابزار اقدام به حمله خودکار با استفاده از حملات Brute-Force در برابر شبکه‌های EAP می‌کند.

```
$ python Auto_EAP.py --help
usage: Auto_EAP.py [-h] -i Interface -s SSID -U Usernamefile -p Password -K
Key_mgmt -E Eap_type

optional arguments:
  -h, --help            show this help message and exit
  -i Interface, --interface Interface
                        The Interface to use
  -s SSID, --ssid SSID The SSID to attack
  -U Usernamefile, --User Usernamefile
                        Path to username file
  -p Password, --password Password
                        Password to use
  -K Key_mgmt, --key_mgmt Key_mgmt
                        Key_Management type to use
  -E Eap_type, --eap_type Eap_type
                        Eap type to use
```

شکل ۴۱ - نمایشی از ابزار Auto_EAP

Bully

این برنامه یک پیاده‌سازی جدید از حملات Brute-force بر روی WPS است که به زبان C نوشته شده است.

```
root@kali:~# bully mon0 -b 00:25:9C:97:4F:48 -e Mandela2 -c 9
[!] Bully v1.0-22 - WPS vulnerability assessment utility
[+] Switching interface 'mon0' to channel '9'
[!] Using '00:c0:ca:3f:ee:02' for the source MAC address
[+] Datalink type set to '127', radiotap headers present
[+] Scanning for beacon from '00:25:9c:97:4f:48' on channel '9'
[+] Got beacon for 'Mandela2' (00:25:9c:97:4f:48)
[!] Creating new randomized pin file '/root/.bully/pins'
[+] Index of starting pin number is '0000000'
[+] Last State = 'NoAssoc' Next pin '96202357'
[+] Sent packet not acknowledged after 3 attempts
[+] Tx( Auth ) = 'Timeout' Next pin '96202357'
[+] Sent packet not acknowledged after 3 attempts
[+] Tx( Auth ) = 'Timeout' Next pin '96202357'
[+] Sent packet not acknowledged after 3 attempts
[+] Tx( M2 ) = 'Timeout' Next pin '96202357'
[+] Rx( ID ) = 'Timeout' Next pin '96202357'
[+] Rx(Beacon) = 'Timeout' Next pin '96202357'
[+] Sent packet not acknowledged after 3 attempts
[+] Tx(DeAuth) = 'Timeout' Next pin '96202357'
```

شکل ۴۲ - نمایی از ابزار Bully

coWPAtty

پیاده‌سازی یک حمله سریع با استفاده از فرهنگ لغت آفلاین به شبکه WPA / WPA2 با استفاده از احراز هویت مبتنی بر PSK.

```
thallium cowpatty $ john --rules --wordlist=../dict/big-dict --stdout | ./cowpa
tty -r wpapsk-linksyst.dump -f - -s linksys
cowpatty 4.0 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA/PSK passphrase.
Starting dictionary attack. Please be patient.
Using STDIN for words.
key no. 1000: !aliquot
key no. 2000: !exotica
key no. 3000: !pelican
key no. 4000: !verbena
key no. 5000: "asdngurg
key no. 6000: "ensimm{isten
key no. 7000: "instituutissa
```

شکل ۴۳ - نمایی از ابزار coWPAtty

Fern Wifi Cracker

Fern Wifi Cracker یک برنامه متمیزی امنیتی بی سیم و همچنین برای نفوذ به این شبکه طراحی شده است که توانایی شکستن و بازیابی پورد های WEP/WPA/WPS را دارد. لازم به ذکر است که این برنامه قابلیت انجام سایر حملات دیگر را بر روی شبکه های بی سیم یا شبکه های اترنت را دارا است.



شکل ۴۴ - تصویری از ابزار Fern Wifi Cracker

Fluxion

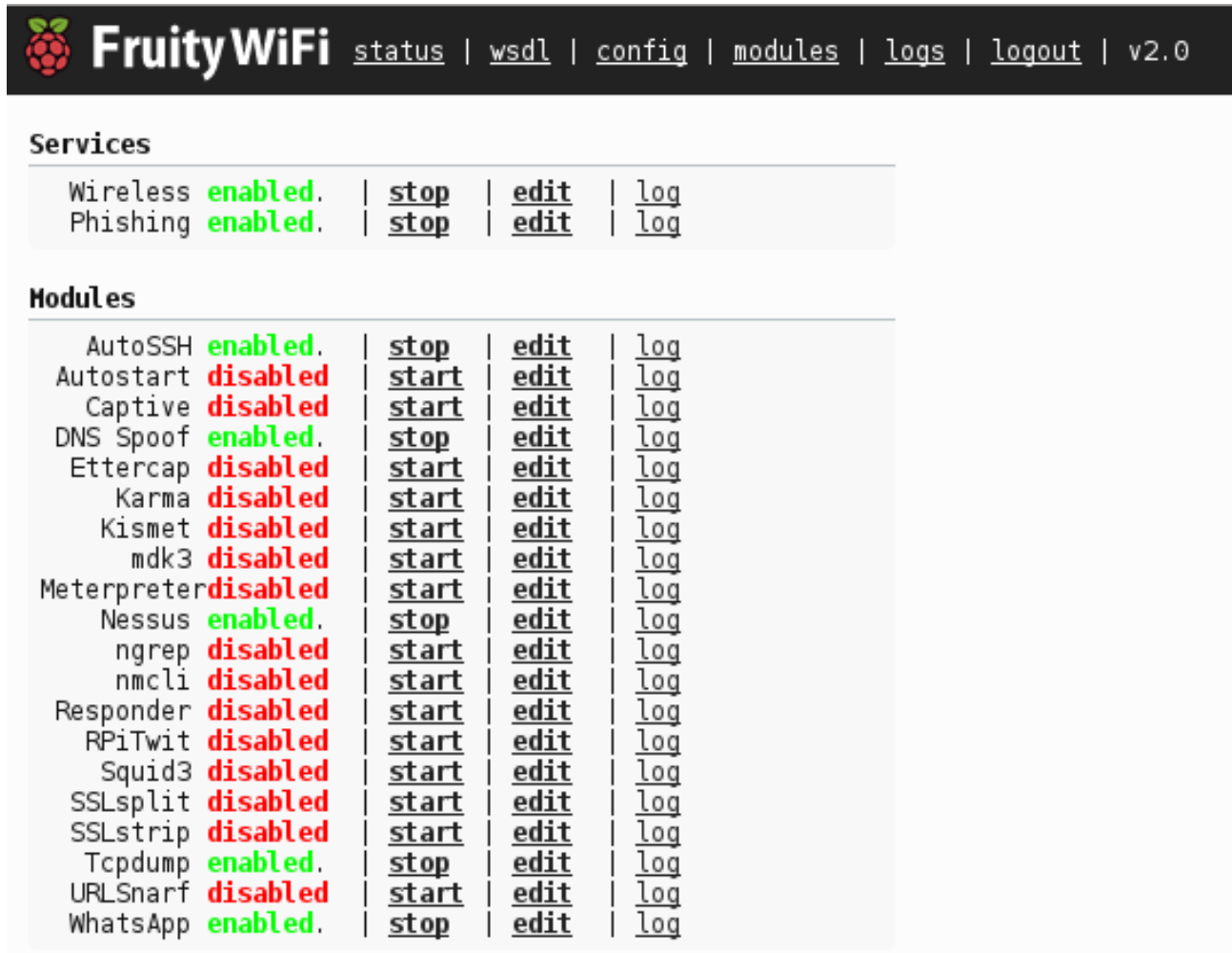
یک ابزار حسابرسی امنیتی و تحقیقات مهندسی اجتماعی است که می تواند حملات MITM WPA را انجام دهد.



شکل ۴۵ - تصویری از ابزار Fluxion

FruityWiFi

یک ابزار س‌ورس باز برای بررسی شبکه‌های بی‌سیم است. این برنامه به کاربر اجازه می‌دهد تا به‌طور مستقیم با استفاده از رابط وب و یا ارسال پیام به این شبکه‌ها حمله‌های پیشرفته را انجام دهد. ابتدا برنامه برای استفاده با Raspberry-Pi ایجاد شد، اما می‌توان آن را بر روی هر سیستم مبتنی بر دبیان نصب کرد.



The screenshot shows the FruityWiFi web interface. At the top, there is a navigation bar with links for [status](#), [wsdl](#), [config](#), [modules](#), [logs](#), [logout](#), and [v2.0](#). Below the navigation bar, there are two main sections: **Services** and **Modules**.

Services

Wireless	enabled.	stop	edit	log
Phishing	enabled.	stop	edit	log

Modules

AutoSSH	enabled.	stop	edit	log
Autostart	disabled	start	edit	log
Captive	disabled	start	edit	log
DNS SpooF	enabled.	stop	edit	log
Ettercap	disabled	start	edit	log
Karma	disabled	start	edit	log
Kismet	disabled	start	edit	log
mdk3	disabled	start	edit	log
Meterpreter	disabled	start	edit	log
Nessus	enabled.	stop	edit	log
ngrep	disabled	start	edit	log
nmcli	disabled	start	edit	log
Responder	disabled	start	edit	log
RPiTwit	disabled	start	edit	log
Squid3	disabled	start	edit	log
SSLsplit	disabled	start	edit	log
SSLstrip	disabled	start	edit	log
Tcpdump	enabled.	stop	edit	log
URLSnarf	disabled	start	edit	log
WhatsApp	enabled.	stop	edit	log

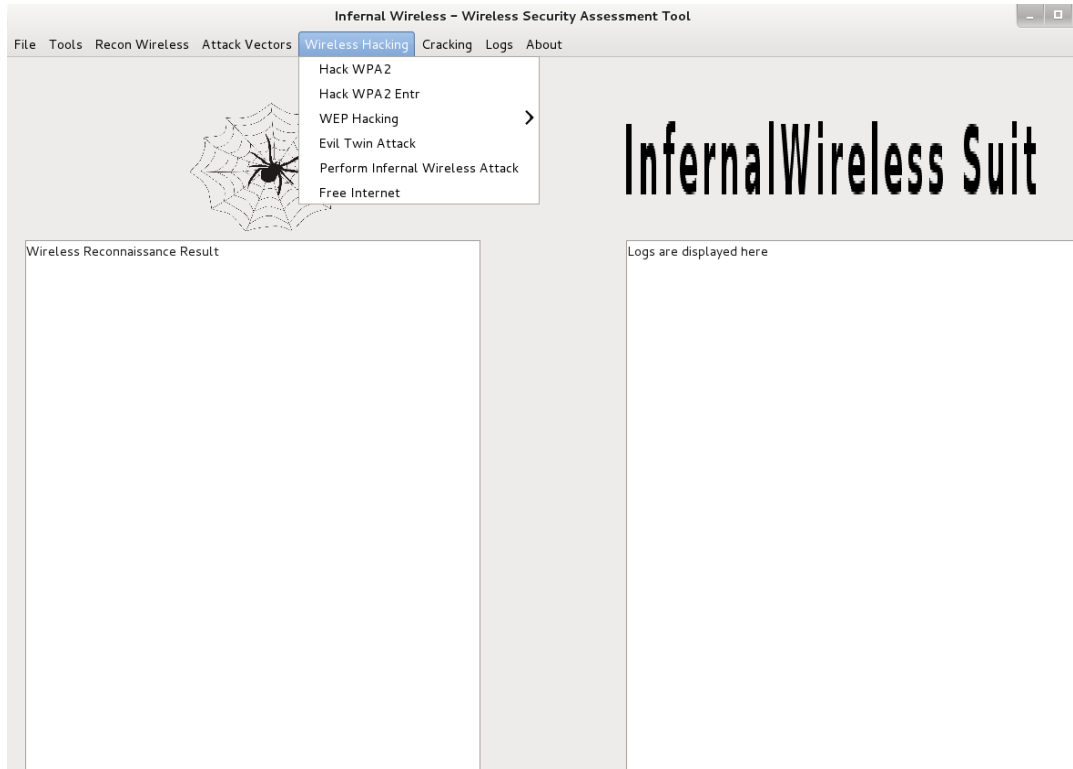
شکل ۴۶ - تصویری از ابزار FruityWiFi

ruityWifi مبتنی بر ماژول‌های انعطاف‌پذیری است. این ماژول‌ها را می‌توان از کنترل پنل نصب کرد تا FruityWifi را با ویژگی‌های جدید ارائه دهد.

در داخل ماژول‌های موجود می‌توانید URLsnarf، DNSspooF، Kismet، mdk3، ngrep، nmap، Squid3 y SSLstrip (قابلیت تزریق کد)، Meterpreter، AutoSSH، Portal Captive و موارد دیگر را پیدا کنید.

Infernal Twin

Infernal Twin یک مجموعه بی نظیر از هک کردن بی سیم است که در پایتون نوشته شده است که بسیاری از وظایف تکراری را که در آزمون امنیتی شبکه‌های WiFi صورت می‌گیرد، خودکار می‌کند. که می‌توان از آن به‌عنوان یک ابزار در عرصه ی پویش آسیب‌پذیری و آزمون نفوذ خودکار بر روی شبکه‌های بی‌سیم نام برد که از تمامی پروتکل‌ها و الگوریتم‌های رمزنگاری پشتیبانی می‌کند و همچنین بعد از اتمام آزمون نفوذپذیری می‌توانید گزارش موارد انجام شده را توسط ابزار انجام دهید.



شکل ۴۷ - تصویری از ابزار Infernal Twin

mdk3

یک ابزار برای بهره‌برداری از ضعف پروتکل IEEE 802.11 است. این برنامه قابلیت انجام حملات Deauthentication و حملات Beacon Request و ... را دارد.

```

-----
##   Choose MDK3 Options   ##
##                       ##
##   1) Deauthentication   ##
##   2) Prob selected AP  ##
##   3) Select another target ##
##   4) Authentication DoS ##
##   5) Return to main menu ##
##                       ##
-----
Option: █

```

شکل ۴۸ - تصویری از ابزار mdk3

PixiewPS

یک ابزار نوشته شده در C برای اتصال به شبکه‌های بی‌سیم از طریق حدس زدن WPS با استفاده از انتروپی کم یا غیرواقعی برخی از مسیرهایها و اکسس پوینت ها

```

~/픽시 wps/pixiewps/src$ ./pixiewps -e d0141b15656e96b85fceed2e8e76330d2b1ac1576bb026e7
a328c0e1baf8cf91664371174c08ee12ec92b0519c54879f21255be5a8770e1fa1880470ef423c90e34d7847a6fcb49
24563d1af1db0c481ead9852c519bf1dd429c163951cf69181b132aea2a3684caf35bc54aca1b20c88bb3b7339ff7d5
6e09139d77f0ac58079097938251dbbe75e86715cc6b7c0ca945fa8dd8d661beb73b414032798dadee32b5dd61bf105
f18d89217760b75c5d966a5a490472ceba9e3b4224f3d89fb2b -r ce733463b55d3c410e59949d94f0b95fff816dc2
cbd27f0832f010121143f37febe96a22e7b43c1a4cce45bbcdfef48a55bcace804c0643286208de9f620c9f8df6b91d1
f1ad7eb9398b49e28ccfa1349dfcb11943a6d6f40fc52c76bedb2fecc516906a4c4fff0c10ae337ef9f82e9aa4b695b
3707256b4e13ceea0e19b29e2b35bdfa8e09bd60f2b3ff78e9b3bd2a0a7d97b633a0046134bfc03c18aada6a002c607
09a56191db258025c9249bb0668bfe45078f4aaa32e937fb88a802850bc -s 2fa02bfdbe2fc4010c6c655870cc8fab
b651f930401c61bb23c28a04597f163f -z 2fa02bfdbe2fc4010c6c655870cc8fab651f930401c61bb23c28a04597
f163f -a 06c01b8d83a4b25ea741980e912f59f3687d22d277526f7f12774bdecdbb16e0 -n 6dda2c0103bb286241
69dcac0b4d3d20 --start 01/1970 --end 02/1970

Pixiewps 1.4

[?] Mode:      3 (RTL819x)
[*] Seed N1:   435108 (Tue Jan  6 00:51:48 1970 UTC)
[*] Seed ES1:  435109 (Tue Jan  6 00:51:49 1970 UTC)
[*] Seed ES2:  435109 (Tue Jan  6 00:51:49 1970 UTC)
[*] PSK1:      5741bf2b58842738232205a6db599fd2
[*] PSK2:      5741bf2b58842738232205a6db599fd2
[*] ES1:       5bba59b478b050d96832c2ff744692e6
[*] ES2:       5bba59b478b050d96832c2ff744692e6
[+] WPS pin:   <empty>

[*] Time taken: 0 s 378 ms

```

شکل ۴۹ - تصویری از ابزار PixiewPS

WEPCrack

ک ابزار سوریس باز برای شکستن کلیدهای مخفی WEP 802.11 است.

```

WEP Crack

La clé K à trouver est de longueur 5 octets (40 bits).
Interception des paquets vérifiant Bn (FMS) et Cn (KoreK A_s13) ...
Merci de patienter ...
Supposition K[0] : d3
Supposition K[1] : 4d
Supposition K[2] : b3
Supposition K[3] : ef
Supposition K[4] : 42
K = [ d3 4d b3 ef 42 ] -> clé correcte.

```

شکل ۵۰ - تصویری از ابزار WEPCrack

Wifijammer

با استفاده از این برنامه شما می‌توانید به‌صورت مداوم تمام کاربران متصل به شبکه‌ی وایرلس را مسدود نمایید.

```
[+] wlan1 channel: 1

          Deauthing          ch  ESSID
[*] c0:4a:00:55550000e - b8:3e:59:000055550 - 4 - 3rdFloor
[*] c0:4a:00:000000000 - c4:43:8f:fffffffff - 4 - 3rdFloor
[*] 00:1f:90:000000000 - 40:0e:85:555500000 - 11 - 6C956
[*] 00:26:62:300000000 - 10:08:b1:000000000 - 11 - SpenglerNet
[*] 00:26:62:300000000 - 14:49:e0:000000000 - 11 - SpenglerNet
[*] 6c:ad:f8:000000000 - c0:4a:00:000000000 - 10 - 1stFloor

          Access Points      ch  ESSID
[*] 00:0d:67:fffffffff - 1 - TWCWiFi
[*] 00:0d:67:fffffffff - 1 - xfinitywifi
[*] fb:d7:66:66666666e - 1 - TWCWiFi
[*] 00:0d:67:fffffffff - 1 - CableWiFi
[*] 00:0d:67:fffffffff - 1 -
[*] 98:0d:67:000000000 - 1 - opvzumwifi
[*] 00:12:c7:fffffffff - 1 - optimumwifi
[*] c0:4a:00:000000000 - 4 - 3rdFloor
[*] a0:21:b7:000000000 - 3 - Nottinghamnetwork.
[*] 00:7f:28:000000000 - 6 - MKK25
[*] 00:1d:7e:000000000 - 6 - AWHODAT
[*] 00:26:62:000000000 - 6 - NGNI6
[*] 6d:91:32:fffffffff - 6 - Plex
[*] 00:24:b2:000000000 - 6 - Plex
[*] 00:7f:28:000000000 - 6 - MKK25
[*] 02:3b:0a:000000000 - 6 - MKK25
```

شکل ۵۱ - تصویری از ابزار Wifijammer

Wifiphisher

از این ابزار جهت انجام حملات فیشینگ به‌صورت خودکار استفاده می‌شود.

```

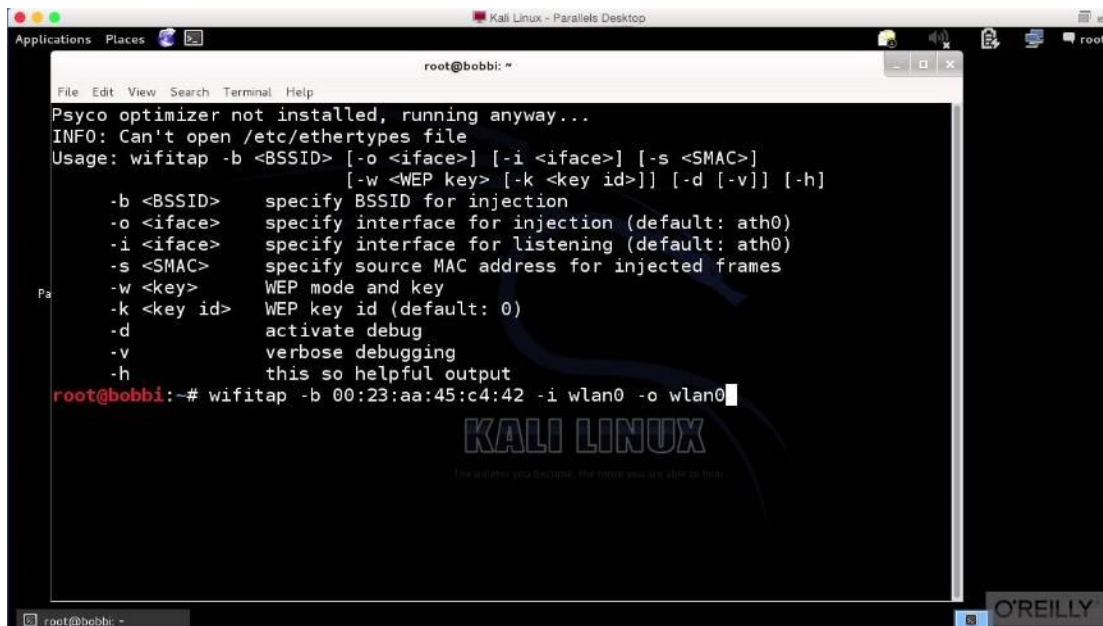
usage: wifiphisher.py [-h] [-c CHANNEL] [-s SKIP] [-jI JAMMINGINTERFACE]
                    [-aI APINTERFACE] [-m MAXIMUM] [-n] [-t TIMEINTERVAL]
                    [-p PACKETS] [-d] [-a ACCESSPOINT]

optional arguments:
  -h, --help            show this help message and exit
  -c CHANNEL, --channel CHANNEL
                        Choose the channel for monitoring. Default is channel
                        1
  -s SKIP, --skip SKIP  Skip deauthing this MAC address. Example: -s
                        00:11:8B:33:44:AA
  -jI JAMMINGINTERFACE, --jamminginterface JAMMINGINTERFACE
                        Choose monitor mode interface. By default script will
                        find the most powerful interface and starts monitor
                        mode on it. Example: -jI mon5
  -aI APINTERFACE, --apinterface APINTERFACE
                        Choose monitor mode interface. By default script will
                        find the most powerful interface and starts monitor
                        mode on it. Example: -jI mon5
  -m MAXIMUM, --maximum MAXIMUM
                        Choose the maximum number of clients to deauth.List of
                        clients will be emptied and repopulated afterhitting
                        the limit. Example: -m 5
  -n, --noupdate        Do not clear the deauth list when the maximum (-m)
                        numberof client/AP combos is reached. Must be used in
                        conjunctionwith -m. Example: -m 10 -n
    
```

شکل ۵۲ - تصویری از ابزار Wifiphisher

Wifitap

این برنامه ارتباط با استفاده از حملات تزریق ترافیک سعی در ایجاد ارتباط با شبکه می‌کند.



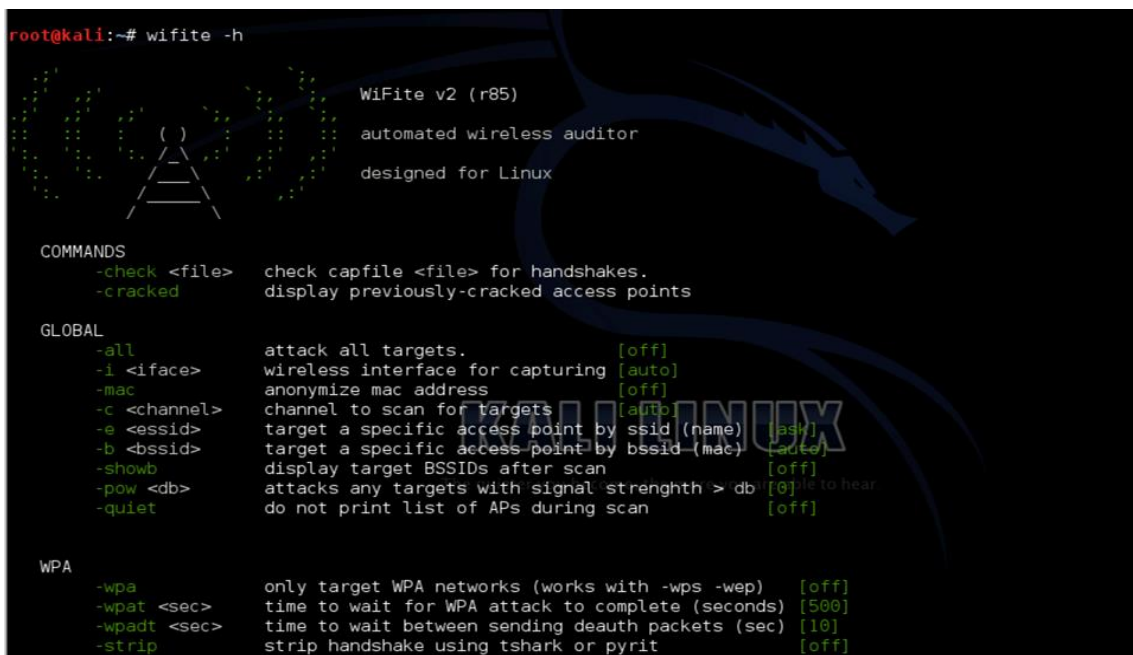
```

root@bobbi:~# wifitap -h
Psycho optimizer not installed, running anyway...
INFO: Can't open /etc/ethertypes file
Usage: wifitap -b <BSSID> [-o <iface>] [-i <iface>] [-s <SMAC>]
        [-w <WEP key> [-k <key id>]] [-d [-v]] [-h]
-b <BSSID>    specify BSSID for injection
-o <iface>    specify interface for injection (default: ath0)
-i <iface>    specify interface for listening (default: ath0)
-s <SMAC>    specify source MAC address for injected frames
-w <key>     WEP mode and key
-k <key id>  WEP key id (default: 0)
-d           activate debug
-v           verbose debugging
-h           this so helpful output
root@bobbi:~# wifitap -b 00:23:aa:45:c4:42 -i wlan0 -o wlan0
    
```

شکل ۵۳ - تصویری از ابزار Wifitap

Wifite

از این ابزار جهت حمله به چندین شبکه رمزگذاری شده WEP، WPA و WPS در یک ردیف استفاده می‌شود.



```

root@kali:~# wifite -h
WiFiFite v2 (r85)
automated wireless auditor
designed for Linux

COMMANDS
-check <file> check capfile <file> for handshakes.
-cracked      display previously-cracked access points

GLOBAL
-all         attack all targets. [off]
-i <iface>    wireless interface for capturing [auto]
-mac         anonymize mac address [off]
-c <channel> channel to scan for targets [auto]
-e <ssid>     target a specific access point by ssid (name) [psk]
-b <bssid>    target a specific access point by bssid (mac) [adcc]
-showb       display target BSSIDs after scan [off]
-pow <db>    attacks any targets with signal strength > db [0] (able to hear)
-quiet       do not print list of APs during scan [off]

WPA
-wpa         only target WPA networks (works with -wps -wep) [off]
-wpat <sec>  time to wait for WPA attack to complete (seconds) [500]
-wpadt <sec> time to wait between sending deauth packets (sec) [10]
-strip       strip handshake using tshark or pyrit [off]
    
```

شکل ۵۴ - تصویری از ابزار Wifite

Zizania

این برنامه با اسنیف ترافیک شبکه‌ی وایرلس برای فایل‌های رمزگزاری شده wpa می‌کند و تنها آن فریم‌های مناسب برای رمزگشایی را مانند EAPOL frames, data.one beacon, و ... را دامپ می‌کند که به صورت شفاف مقادیر را منتشر می‌کند. همچنین این برنامه جهت بالا بردن فرآیند یک فریم DeAuth از استاندارد IEEE 802.11 به صورت مکرر به ایستگاه کاری که به handshake او را نیاز دارد ارسال می‌کند.

```

bash
$ zizania -v -r wpa-Induction.pcap -w out.pcap
[*] User not root, nothing to do
[*] Dumping packets to 'out.pcap'
[*] Starting the dispatcher thread
[+] Parsing 'wpa-Induction.pcap'
[+] BSS discovered 'Coherer' (00:0C:41:82:B2:55)
[*] 5.650 - 00:00:93:82:36:3A @ 00:0C:41:82:B2:55 - Handshake message #1 (first attempt detected)
[+] New client 00:00:93:82:36:3A @ 00:0C:41:82:B2:55
[*] 5.651 - 00:00:93:82:36:3A @ 00:0C:41:82:B2:55 - Handshake message #2
[*] 5.656 - 00:00:93:82:36:3A @ 00:0C:41:82:B2:55 - Handshake message #3
[*] 5.656 - 00:00:93:82:36:3A @ 00:0C:41:82:B2:55 - Handshake message #4
[+] ^ ^ Full handshake for 00:00:93:82:36:3A @ 00:0C:41:82:B2:55
[+] New client 00:00:1D:06:E0:F2 @ 00:0C:41:82:B2:55
[*] EOF for 'wpa-Induction.pcap'
[*] Terminating due to signal 15
[+]
[+] SSID 'Coherer' (00:0C:41:82:B2:55)
[+] - Handshakes ..... 1
[+] - Stations ..... 1
[+] - Data packets ... 144
[+] Decrypt with airdecap-ng -e 'Coherer' -b 00:0C:41:82:B2:55 -p '?' 'out.pcap'
[+]
[+] SSID '' (98:D3:04:64:FA:55)
[+] - Handshakes ..... 0
[+] - Stations ..... 0
[+] - Data packets ... 0
[*] Closing packet dump 'out.pcap'
$
    
```

شکل ۵۵ - تصویری از ابزار Zizania

FakeAP

همانطور که از اسم برنامه پیداست با استفاده از این برنامه می‌توانید یک Acces point جعلی ایجاد کنید.

```

root@kali: ~
File Edit View Search Terminal Help
wsf > use network/fakeap
[!]Notice : You Should Be Installed DHCP Before Run This Attack, If DHCP Not Ins
talled Run This Command :
sudo apt-get install dhcp3-server
wsf:Fake_AP > show options

Options          Value          RQ      Description
-----
Interface        wlan0          yes     Wireless Interface Name
ESSID            FakeAP        yes     ESSID Name For Fake AP
Channel          11            yes     Channel Number

wsf:Fake_AP > set ESSID Free-Internet
ESSID => free-internet
wsf:Fake_AP > show options

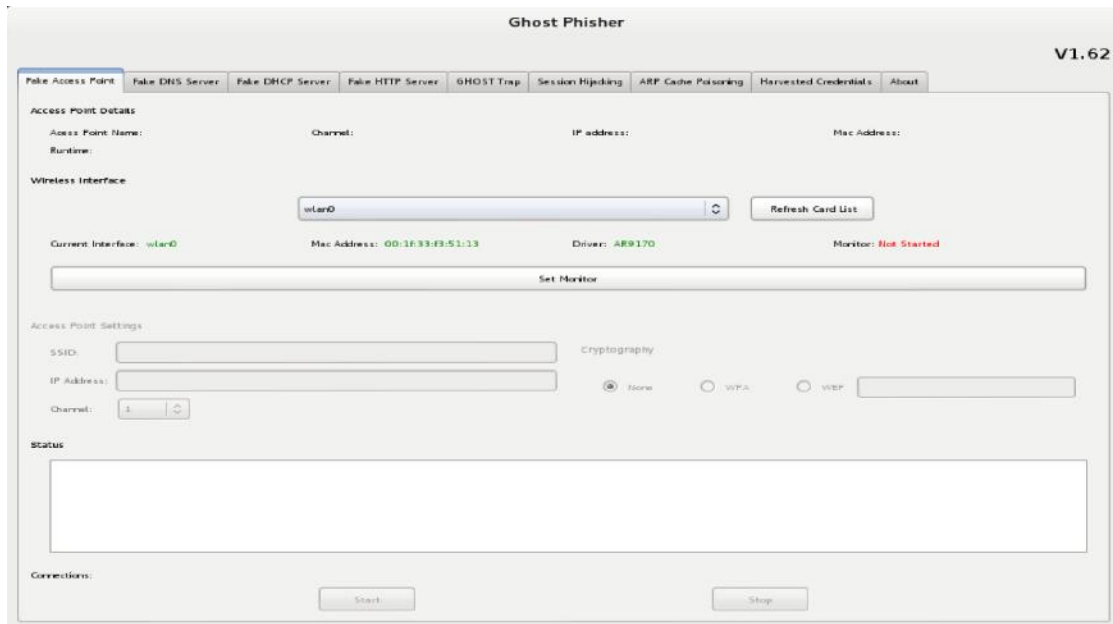
Options          Value          RQ      Description
-----
Interface        wlan0          yes     Wireless Interface Name
ESSID            free-internet  yes     ESSID Name For F
ake AP
Channel          11            yes     Channel Number

wsf:Fake_AP >
    
```

شکل ۵۶ - تصویری از ابزار FakeAP

Ghost Phisher

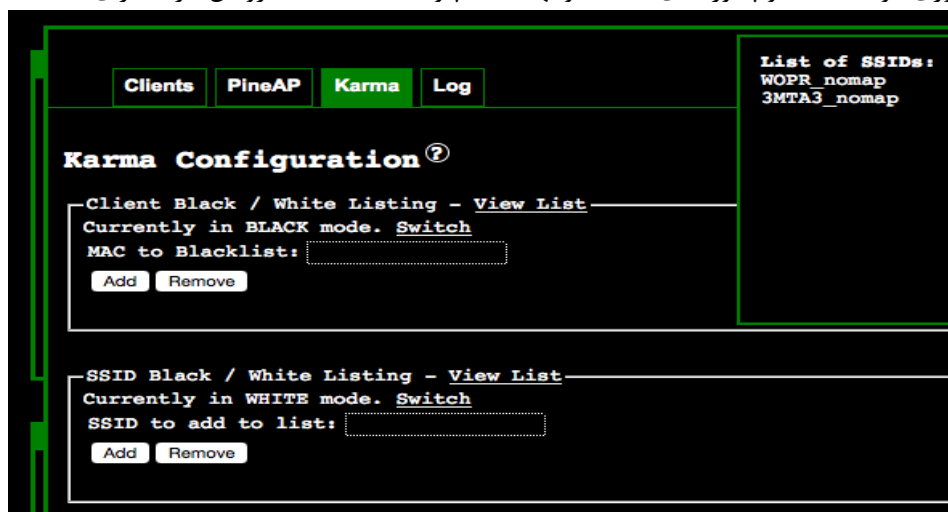
برنامه ghost Phisher ی برنامه ممیزی امنیتی بی سیم و شبکه‌ی اترنت و همچنین برنامه ای جهت آزمون میزان نفوذپذیری این شبکه‌ها است که به زبان پایتون و کتابخانه های QT پایتون نوشته شده که به ما امکان ایجاد AP جعلی و انجام بسیاری دیگر از حملات جعل سرویسها و ... است که برای حملات مهندسی اجتماعی می تواند بسیار مفید باشد.



شکل ۵۷ - تصویری از ابزار Ghost Phisher

Karma

KARMA مجموعه‌ای از ابزارها برای ارزیابی امنیت مشتریان بی سیم در چند لایه است. ابزارهای استراق سمع به شناسایی کاربران کاربران موجود و همچنین شبکه‌های مرجع و قابل اعتماد را با گوش دادن به فریم‌های مربوط به درخواست probe در استاندارد ۸۰۲.۱۱ می پردازد. از آنجاکه مشتریان فردی می توانند با ایجاد یک Rogue AP در داخل شبکه تهدید شوند و یا توسط یک دراپور به درخواست Probe پاسخ دهند و از این کار جهت درخواست اتصال به تمام SSID های در دسترس استفاده نماید. سرویس های جعلی سطح بالا می توانند به جمع آوری گواهینامه ها و پسوردهای مختلف و نهائینا اکسپلویت هاب سمت سرویس گیرنده برای هاست استفاده کرد



شکل ۵۸ - تصویری از ابزار Karma

mitmAP

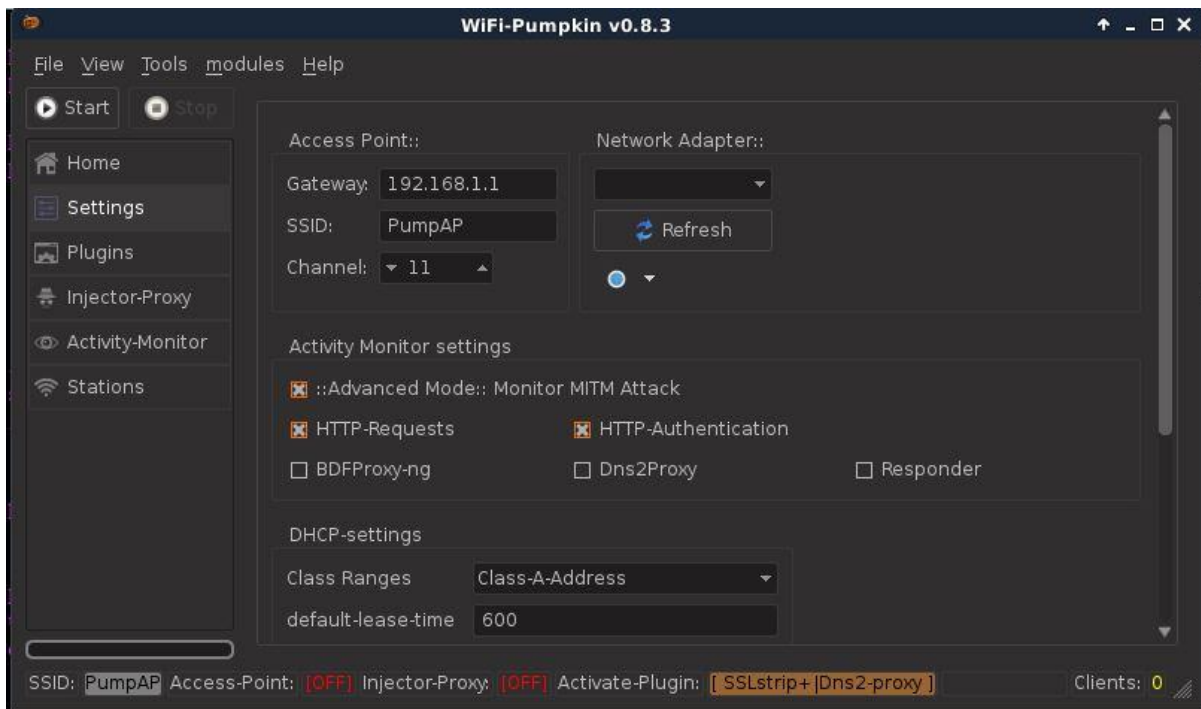
این برنامه نوشته شده به زبان پایتون که به منظور ایجاد یک نقطه‌ی اتصال جعلی و استراق سمع در آن به کار برده می‌شود.



شکل ۵۹ - تصویری از ابزار mitmAP

WiFi-Pumpkin

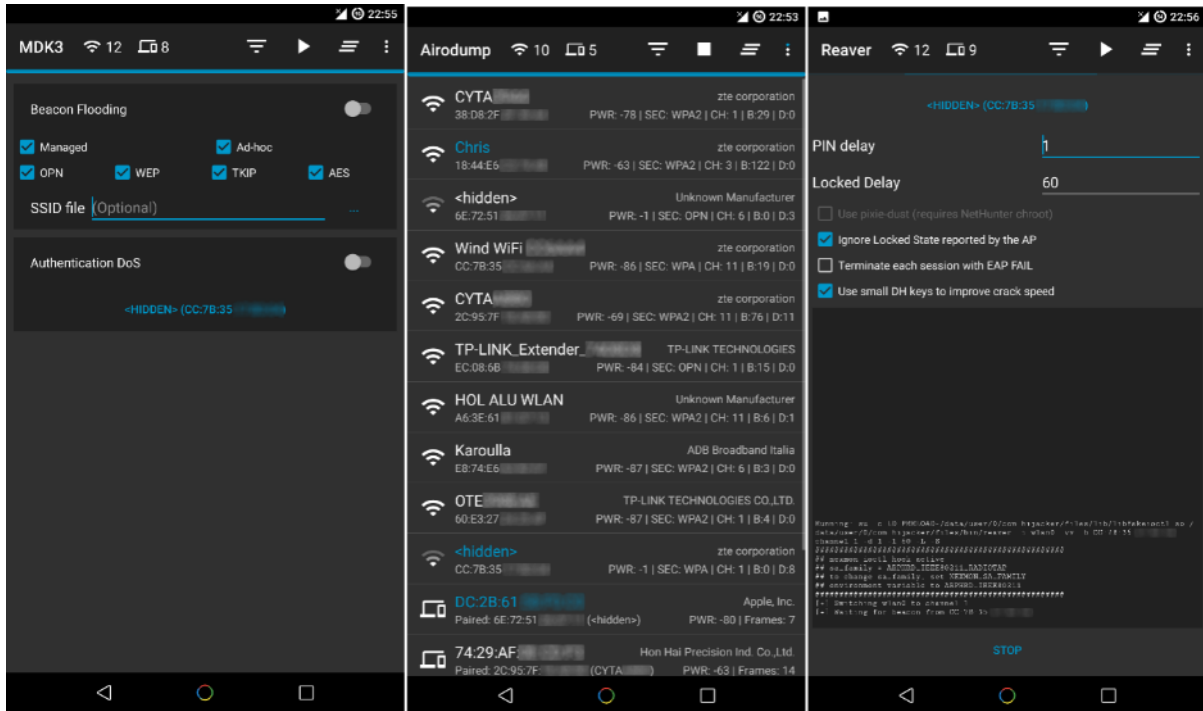
این برنامه دارای یک چارچوب بسیار کامل برای حسابرسی امنیت Wi-Fi است. ویژگی اصلی این است که توانایی ایجاد AP جعلی و ایجاد حمله مردانه در میان، اما لیست ویژگیها بسیار گسترده است. از ویژگی‌های اصلی آن می‌توان به ایجاد نقطه اتصال از نوع Rogue، حملات Deauth، درخواست Probe، حملات DHCP Starvation، حملات Windows Update، حملات DNS Spoof و ... اشاره کرد.



شکل ۶۰ - تصویری از ابزار WiFi-Pumpkin

Hijacker

Hijacker یک رابط کاربر گرافیکی برای ابزارهای آزمون نفوذ Aircrack-ng، Airodump-ng، MDK3 و Reaver برای پلتفرم اندروید است. این یک UI ساده و آسان را برای استفاده از این ابزار بدون تایپ کردن دستورات در کنسول و کپی کردن و چسباندن آدرس های MAC ارائه می دهد.



شکل ۶۱ - تصویری از ابزار Hijacker

<https://www.sans.org/course/wireless-penetration-testing-ethical-hacking>
<https://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks>
[/https://www.concise-courses.com/hacking-tools/wireless-tools](https://www.concise-courses.com/hacking-tools/wireless-tools)
[/https://fossbytes.com/best-wifi-hacking-software-analysis-tools-computer](https://fossbytes.com/best-wifi-hacking-software-analysis-tools-computer)
<https://www.techworm.net/2018/01/10-best-wi-fi-hacking-tools-2018.html>
[/www.subliminalhacking.net/2013/02/07/wireless-attack-and-audit-tools-recommendations-list](http://www.subliminalhacking.net/2013/02/07/wireless-attack-and-audit-tools-recommendations-list)
[/http://resources.infosecinstitute.com/13-popular-wireless-hacking-tools](http://resources.infosecinstitute.com/13-popular-wireless-hacking-tools)
[/https://phoenixts.com/blog/types-of-wireless-network-attacks](https://phoenixts.com/blog/types-of-wireless-network-attacks)
<https://www.examcollection.com/certification-training/security-plus-wireless-attacks-and-their-types.html>
<https://www.symantec.com/connect/articles/wireless-attacks-and-penetration-testing-part-1-3>
<https://www.sans.org/reading-room/whitepapers/detection/understanding-wireless-attacks-detection-1633>
<http://bytegate.ir/%D9%BE%D8%B1%D9%88%D8%AA%DA%A9%D9%84-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-wep-%DA%86%DB%8C%D8%B3%D8%AA%D8%9F-%DA%86%D8%B1%D8%A7-%D9%82%D8%A7%D8%A8%D9%84-%D9%87%DA%A9-%D8%A7%D8%B3%D8%AA%D8%9F>
<https://lirias.kuleuven.be/bitstream/123456789/401042/1/wpatkip.pdf>
https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#Security_issues
<https://www.mojonetworks.com/wpa2-hole196-vulnerability>
<https://apa.aut.ac.ir/?p=3110>
<https://www.winncom.com/en/glossary>
https://www.juniper.net/documentation/en_US/junos-space-apps/network-director2.0/topics/concept/wireless-ssid-bssid-ssid.html
searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks
<https://packetstormsecurity.com/papers/wireless>
[/https://www.darknet.org.uk/2017/09/reaver-download-hack-wps-pin-wifi-networks](https://www.darknet.org.uk/2017/09/reaver-download-hack-wps-pin-wifi-networks)
[/https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-psk-passwords-with-cowpatty-0148423](https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-psk-passwords-with-cowpatty-0148423)
[/witestlab.poly.edu/blog/802-11-wireless-lan-2](http://witestlab.poly.edu/blog/802-11-wireless-lan-2)
<https://www.slideshare.net/shreejanacharya/ieee80211-wireless-network>
www.securitytube.net/groups?operation=view&groupId=9
[/https://www.wired.com/story/krack-wi-fi-wpa2-vulnerability](https://www.wired.com/story/krack-wi-fi-wpa2-vulnerability)

https://en.wikipedia.org/wiki/Cracking_of_wireless_networks

resources.infosecinstitute.com/20-popular-wireless-hacking-tools-updated-for-2016

[/https://www.cybrary.it/0p3n-category/wireless-hacking-and-security](https://www.cybrary.it/0p3n-category/wireless-hacking-and-security)

<https://www.sanog.org/resources/sanog6/peterson-poudel-wireless-archi-tutorial.pdf>

<https://www.louiewong.com/archives/407>Penetration Testing: A Hands-On Introduction to Hacking By Georgia Weidman

Hacking Wireless Networks – The ultimate hands-on guide By Andres k. Kolokothas

WarDriving & Wireless Penetration Testing By Chris Hurley, Russ Rogers, Frank Thornton