

- اتصال الواي فاي سهل ولكن غير آمن
- ارتكاب الاكاذيب صعب ولكن أمن (no sniffing).^٦

مصطلحات لاتصال الانترنت اللاسلكي **Wireless**



	Bandwidth كمية البيانات المستهلكة في الاتصال		Wi-Fi HOTSPOT Hotspot عندما يكون الواي فاي على الأجهزة غير المترسبة		GSM نظام عالمي يستخدم في الجوال لتلقي شبكات التصال الواي فاي في العالم
	عملية التصال جهاز الواي فاي في Access point		تستخدم للاتصال جهاز الواي فاي في شبكة الواي فاي اللاسلكية		SSID = MAC MAC Address for access point setup a Basic Service Set (BSS)

Wireless	مزايا	Wireless	مزايا
سرعة وسهولة التثبيت والتنويع غير الأسطواني	بسهولة وأمان على مختلف الأجهزة	تعزيز حرارته في التربيب حيث تصل إلى أعلى مما يمكن استخدامه	سرعة وسهولة التثبيت والتنويع غير الأسطواني

أساسيات شبكة اللاسلكية **Wireless**

Range (ft)	Speed (Mbps)	Modulation	Freq (GHz)	
27 - 25	54	OFDM	5	802.11a
150 - 150	11	DSSS	2.4	802.11b
150 - 150	54	OFDM , DSSS	2.4	802.11g
Defines WPA2-Enterprise/WAP2-Personal for Wi-Fi				802.11i
~100	54	OFDM	2.4 , 5	802.11n
30 miles	70 - 1000		10 - 66	802.16 (WiMAX)
25	1 - 3		2.4	Bluetooth

Wi-Fi Chalking

WarDriving	WarFlying	WarChalking	WarWalking

يتغول المخترق في السيارة حول شبكات الانترنت ويحاول الاتصال من الاینترنت للتعرف على الشبكات اللاسلكية المفتوحة ، واي فاي.

أنواع الشبكات اللاسلكية Wireless	Bluetooth	Wimax	Wifi
تحتوى Wireless بخلاف WiFi على العديد من المطارات و WiFi يعتمد على Direct sequence Frequency Hopping	هو بسيط في حد ذاته لكن المطارات و وسائل الاعلام WiFi و WiFi يعتمد عليه بدل WiFi	هو بسيط في حد ذاته لكن المطارات و وسائل الاعلام WiFi و WiFi يعتمد عليه بدل WiFi	هو بسيط في حد ذاته لكن المطارات و وسائل الاعلام WiFi و WiFi يعتمد عليه بدل WiFi

Service Set Identifier (SSID)

- هو عبارة عن رقم Token يدخل عن طريق المتصفح على جهاز الواي فاي .
- تعمل على انبعاث الرد الشفاف بين المتصفح والمستخدم
- هي عبارة عن رقم يدخل عن طريق المتصفح على جهاز الواي فاي .
- هي عبارة عن رقم يدخل عن طريق المتصفح على جهاز الواي فاي .
- هي عبارة عن رقم يدخل عن طريق المتصفح على جهاز الواي فاي .
- هي عبارة عن رقم يدخل عن طريق المتصفح على جهاز الواي فاي .
- هي عبارة عن رقم يدخل عن طريق المتصفح على جهاز الواي فاي .
- هي عبارة عن رقم يدخل عن طريق المتصفح على جهاز الواي فاي .

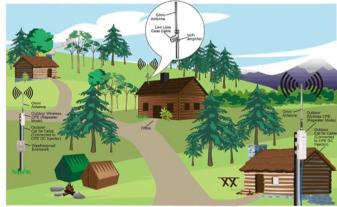
Basic Service Set ID (BSSID)



أنواع الشبكات اللاسلكية الهوائية

Omni-directional

يُوفِر 360 درجة بـشكل دائري موجات تستخدَم محطة أساسية للاتصال اللاسلكي



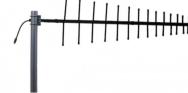
Directional Antennas

تستخدَم لبث موجات الراديو من اتجاه واحد



Yagi Antenna

هو بث المدى الأبعد يُصدِّق على نطاق أقصى ممكن 10 MHz to VHF and UHF



Parabolic Grid

طبق قوي يستخدم لبث معلم ضيق في المدى، يُقدِّم نطاقً موجات راديو في حدود 10 ميل متر وذيل



أنواع الشبكات اللاسلكية الهوائية



السمات				التشفير
سلامة فحص الاتصال	طول مفتاح التشفير	IV حجم	خوارزميات التشفير	
CRC-32	bit-40/104	bits-24	RC4	WEP
Michael Algorithm and CRC-32	bit-128	bits-48	RC4, TKIP	WPA
CBC-MAC	bit-128	bits-48	AES-CCMP	WPA 2

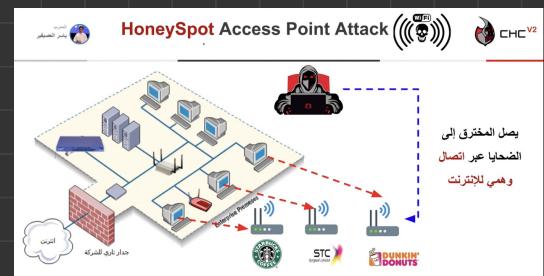
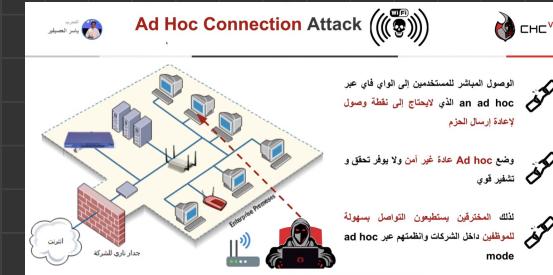
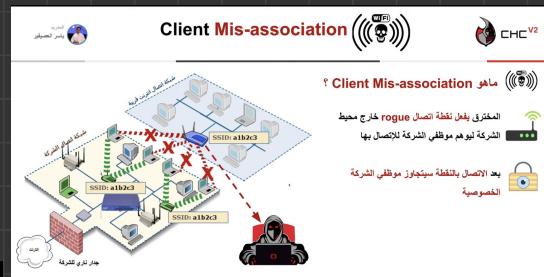
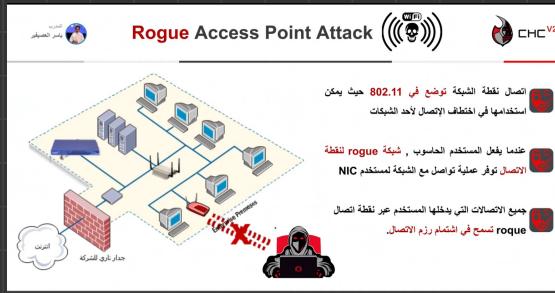
الأسرار رفتك
ك دكتور

موجه بالأجهزة حالياً
وهو من

كيفية فك تشفير اتصال WEP



HACKER					
شقل ادوات كراكر مثل Cain & Abel or Aircrack-ng لإستخراج مفتاح IVs التشفير من	ابداً بعمل تشفير لحزم الواي فاي مثل Aireplay-ng in ARP واطلب اعادة واتطلب اعادة للحزم Inject	ابداً يعمل على الواي فاي باستخدام أدوات مثل airodump-ng or Cain & Abel لجمع بيانات IVs	أبداً يعملي على الواي فاي على الواي فاي باستخدَم أدوات مثل aireplay-ng لعمل تحقُّق وهى مع نقطة الاتصال	استخدَم أداة مثل أداة aireplay-ng لاختبار قابلية الـ Injection لجهاز الوايبرس لنقطة الاتصال	تشغيل واجهة Wireless إلى وضع التحكم في قناة اتصال معينة



Use aircrack to crack WEP networks

طرق اختراق شبكة Wireless



طرق الوصول إلى شبكة الواي فاي للحصول على مخول غير مصرح به على مصادر الشبكة.



الوصول إلى شبكة Wi-Fi



Wifi تشفير



Wireless (الاتصال اللاسلكي)



تحليل الاتصال والبيانات



عمل ملطف GPS



البحث والاستكشاف

الاتصال

Wireless

Footprint the wireless network



الهجم على شبكة الاتصال اللاسلكي تبدأ باكتشاف و جمع المعلومات عن شبكة الاتصال اللاسلكي في الطريقتين active and passive

Passive Footprinting

المهاجم يستخدم طريقة سليمة للتعرف على نقاط الاتصال الانترنت
بواسطة الاستماع على رقم البيانات من الموجات الهوائية، التي
تُسكن نقاط الاتصال اللاسلكية في الشبكة، مثل SSID و جهاز الواي فاي



المهاجم يعلم الشبكة على رقم البيانات في الشبكة

Active Footprinting

جهة المهاجم يرسل استعلامات مع SSID لمعرفة رد فعله
الاتصال، لو وجده الواي فاي لا ينطوي على SSID في البداية إذا
سوف ترسل استعلامات مع رقم SSID



المهاجم يرسل استعلام تجاه

البحث عن اتصال شبكة Wi-Fi للإختراق



أدوات يمكن استخدامها:

inSSIDer , Vistumbler , NetStumbler , NetSurveyor



برنامح للتعرف على الواي فاي



الاتصال هواي خارجي



لaptop مع كارد واي فاي

اكتشاف شبكات الاتصال اللاسلكي



التسجيل في برنامج WIGLE وتحميل خريطة المنطقة وعرض نقاط الاتصال على الخريطة	1
اتصال بجهاز الهوائي (GPS) في الاتوب عبر USB	2
ثبت برنامج NetStumbler وتنشئ على جهاز GPS	3
قود السيارة بسرعة 35 mph or below 35 قود السيارة بسرعة 35 mph or below 35	4
اتصل الواي فاي في المكان الذي تختاره في NetStumbler	5
ارتفاع الملف على برنامج WIGLE ، وبشكل تلقائي سوف تعرّف لك نقاط الاتصال على الـ GPS Access point	6

الحماية ضد اختراق الاتصال اللاسلكي

Wireless



التحقق للأمان	SSID ضبط إعدادات	خطوات الحماية الصحيحة للشبكة
<ul style="list-style-type: none"> استخدم نقطة وصول أمنة WPA2 بدلاً من WEP ابعد جميع التعريفات للشبكات اللاسلكية للأجهزة محدثة دائمة ضع نقطة الاتصال اللاسلكي في مكان آمن استخدم ملء مرآقي للتحقق عزل الشبكة في حال عدم الحاجة في استخدامها 	<ul style="list-style-type: none"> استخدم SSID cloaking لحظ بعض لا يستخدم SSID اسم الشركة او اسم الشبكة او أي كلمات سهلة تخمينها جعل الفتحات الداجر الذكي بين الوصول و الشبكة الآمنة تغطى التحقق كل قترة من جهاز الاتصال اللاسلكي IPSEC over wireless 	<ul style="list-style-type: none"> تغيير الإفراطي لـ SSID بعد الانتهاء من WLAN. إيقاف الاتصال والدخول عن بعد في الرواير لحساب المدير. تغطى فتحة MAC Address في نقطة الوصول والرواق ، مما يمنع إدخال حركة تغطى التحقق في نقطة الوصول إيقاف بث SSID ، مما يزيل كل معلومات الاتصال والبيانات المقدمة من المدخل تضليل زمرة البيانات مثل

