جامعة القدس المفتوحة

الدليل العملي المقترح

مقرر امن الشبكات اللاسلكية

كلية التكنولوجيا والعلوم التطبيقية

اعداد : أ. عصام حطاب
طولكرم
2023

المقدمة

كما تعلم عزيزي الدارس ان تحقيق الامن يعتبر ضرورة ملحة في كل انواع شبكات الحاسوب . الا ان اهميته تزداد بشكل اكبر في شبكات الحاسوب اللاسلكية . يكمن السبب الرئيسي وراء ذلك هو ان الاشارات اللاسلكية لا تحمل و لا تنتقل عبر الاسلاك مما يمكن اي جهاز داخل المجال الذي تغطيه تلك الاشارات من استقبالها بسهولة تمهيدا لاحداث الكوارث والاختراقات الامنية للشبكة.
في الشبكات السلكية يتم تشفير البيانات فقط عند الحاجة لارسالها عبر شبكة عامة غير موثوقة مثل الانترنت في حين لا يتم تشفير سير البيانات بين الاجهزة داخل الشبكة المحلية نفسها . على عكس الشبكات اللاسلكية التي يعتبر تشفير البيانات المنتقلة بين الاجهزة (Clients) و نقطة الولوج (Access Points) ضرورة ملحة.
يحتوي هذا الدليل على مجموعة من المفاهيم الامنية الاساسية والثانوية التي تساعد في توظيف درجات مختلفة من الحماية للشبكات اللاسلكية .كما و يحتوي على مجموعة من الاوامر والطرق التي يستخدمها مهاجموا الشبكات اللاسلكية لشن هجماتهم غير الشرعية لتحقيق اغراض شتى من تنصت وتزوير وتعطيل الخ....
ان الهدف الاساسي لمحتوى هذا الدليل هو تعريف الدارس عمليا بمجموعة من اساليب تامين الشبكات اللاسلكية و تعريفه ايضا ببعض اساليب مخترقوا الانظمة في تنفيذ هجماتهم ضد الشبكات حتى تتكون لديه بعض الامكانات لاختبار امن الشبكات والانظمة وتحديد نقاط الضعف فيها لتامينها. ولا يهدف باي حال الى تعريف اساليب تنفيذ الهجمات من اجل تحقيقها ذاتها. تم تقسيم اجراءات تنفيذ الاوامر والخطوات اللازمة الى جلسات عملية كل منها متعلق بموضوع امني معين.

الاجهزة والمعدات المقترحة اللازمة لتنفيذ جلسات الدليل العملية:

- جهاز حاسوب
- نظام تشغيل ويندوز
- نظام تشغيل Kali Linux يفضل ان يكون مثبت على برمجية الة تخيلية مثل VMware
- جهاز رواتر
- كرت شبكة لاسلكي خارجي(USB Wireless Card)

ارشادات هامة:

- يفضل استخدام راوتر (AP) غير الراوتر المستخدم لشبكتك الحقيقية في البيت خوفا من تنفيذ خطوات تؤدي الى تعطيل شبكة البيت اللاسلكية و بالتالي فقدان اتصال اجهزة البيت بها.
- يمكنك استخدام راوتر ولا حاجة لاتصاله بالانترنت. فتنفيذ مهمات الجلسات العملية اللاحقة لا تستدعي ان يكون الراوتر متصل بالانترنت.
- تذكر ان الهدف الرئيس من جلسات الدليل هو معرفة اساليب تنفيذ الهجمات ضد الشبكات اللاسلكية من اجل تفاديها وليس من اجل تنفيذها.

الجلسة العملية الاولى
Security Fundamentals
(تحقيق وتوظيف المفاهيم الامنية الاساسية لتامين الشبكة اللاسلكية)

وصف الجلسة:

ان الركائز الامنية الاساسية في علم امن المعلومات اللازمة لتحقيق الامن في كل انواع شبكات الحاسوب هي نفسها المطلوبة لتحقيق الامان في الشبكات اللاسلكية. في هذه الجلسة سيتم التعرف على كيفية تحقيق الكثير من المفاهيم الامنية الاساسية والثانوية للمساعدة في تامين الشبكة اللاسلكية وكما تعلم عزيزي الدراس ان الركائز الامنية الاساسية تتمثل في:

- **التحقق من الهوية (Authentication)** والذي يهدف الى التاكد من هوية الجهاز المتصل قبل السماح له بالارتباط بنقطة الوصول(AP). كما يشمل بالنسبة للجهاز التاكد من هوية نقطة الوصول (AP) قبل الاتصال بها خوفا من ان تكون نقطة اتصال مزيفة وخبيثة
- **السرية (Confidentiality)** والتي تهدف الى ضمان ان البيانات المتبادلة بين الجهاز المتصل ونقطة الوصول(AP) غير مقروءة للجميع باستثناء الجهاز المتصل ونقطة الوصول. تشفير البيانات هو اهم الاجراءات المستخدمة لتحقيق ذبك مع الانتباه الى ضرورة استخدام نفس البروتوكول من قبل المرسل والمستقبل والا سيؤدي الى عدم التفاهيم بينهم
- **التكاملية (Integrity)**والتي تهدف الى التاكد من الرسالة المرسلة من المرسل هي نفسها التي استقبلها المستقبل دون حدوث اي تعديل عليها. ومن الاساليب المستخدمة لضمان ذلك هو MIC(Message Integrity /check) الذي يضاف الى الرسالة المرسلة من المرسل.
- **اجراءات امنية اضافية** :يوجد ايضا مجموعة من الاجراءات الامنية التي يمكن تنفيذها للمساعدة في تامين الشبكة اللاسلكية .

في هذه الجلسة سيتم تنفيذ خطوات تطبيق الاجراءات الامنية السابقة على الراوتر لحماية الشبكة اللاسلكية مع الانتباه الى ان هذه الخطوات قد تختلف حسب الراوتر المستخدم.

اهداف الجلسة:

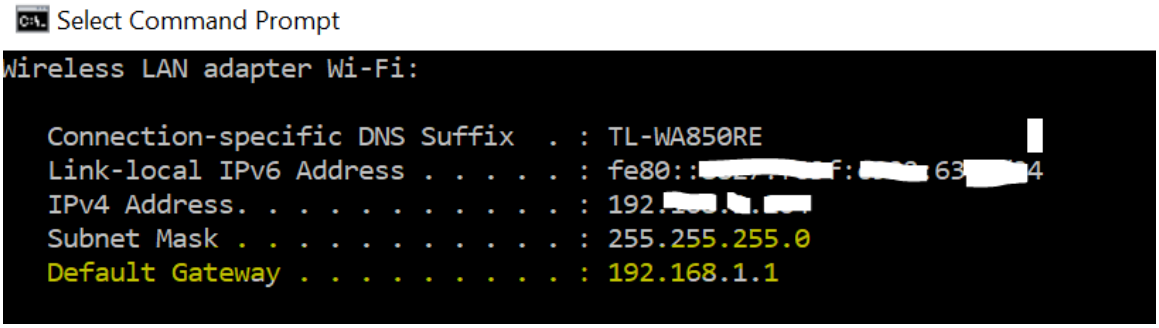
- تطبيق اجراءات الدخول الى الراوتر(والذي يمثل AP ايضا) للتعرف على الية تحقيق المفاهيم الامنية الاساسية المذكورة سابقا في وصف الجلسة.
- تطبيق اجراءات تغيير بيانات الهوية الافتراضية للدخول الى AP: كما تعلم عزيزي الدارس فان بيانات الهوية اللازمة للدخول الى Wireless Router او AP تاتي عادة معه عند شرائه والتي تكون في الغالب مكتوبة على الشريط الخلفي وموحدة للجميع تتمثل في User name: admin و password: admin
- تطبيق اجراءات اخفاء اسم الشبكة اللاسلكية SSID : فيمكن تفعيل خاصية اخفاء اسم الشبكة وبالتالي لا يظهر اسمها عندما يقوم جهاز ما بالبحث عن الشبكات اللاسلكية المحيطة. وتمكين فقط الاجهزة التي تعرف مسبقا اسم الشبكة اللاسلكية من الارتباط بها
- تطبيق اجراءات فلترة العناوين الفيزيائية (MAC Address Filtering) :حيث يمكن تحديد الاجهزة التي سيسمح لها بالارتباط بالشبكة اللاسلكية من خلال عمل قائمة داخل AP بعناوين MAC لتلك الاجهزة ليقبل اتصالها ويرفض الاتصال من غيرها.
- تطبيق اجراء تفعيل الجدار الناري داخل AP: بالاضافة للجدار الناري الخاص بكل جهاز Host Firewall يوجد هناك النوع Network Firewall و الذي يمكن تفعيله بداخل AP ليتحكم باتصالات كل الاجهزة داخل الشبكة.

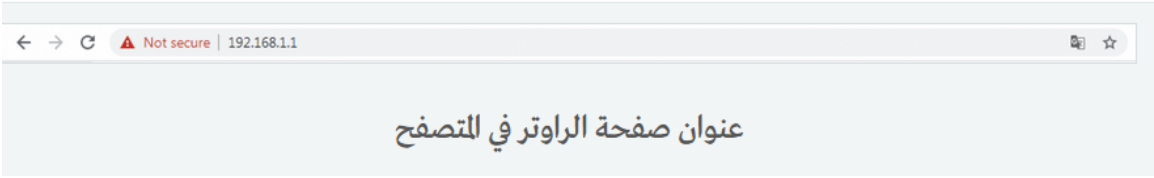
نظام التشغيل المستخدم في تطبيق الجلسة:

Windows 10 Pro او Kali Linux

تطبيق الجلسة:

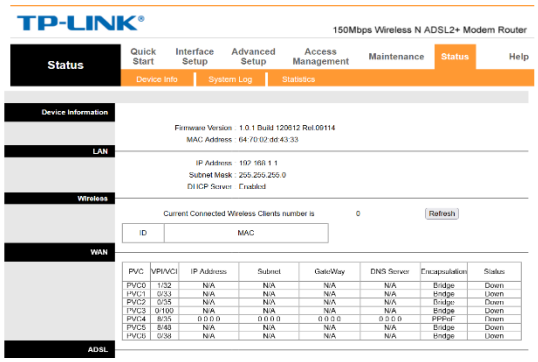
- قم بالاتصال بالراوتر سواء عن طريق كابل أو عن طريق شبكة الواي فاي الخاصة بالراوتر والتي يكون اسمها بالعادة نفس اسم نوع الرواتر مثلا TP-Link
- قم بفتح المتصفح الخاص بجهازك ثم اكتب في شريط العنوان الخاص به عنوان صفحة الراوتر وهو عبارة عن عنوان IP الخاص بالراوتر والتي يمكن معرفته من خلال الامر ipconfig في شاشة موجه الاوامر (عادة يكون 192.168.1.1) كما في الصورة:



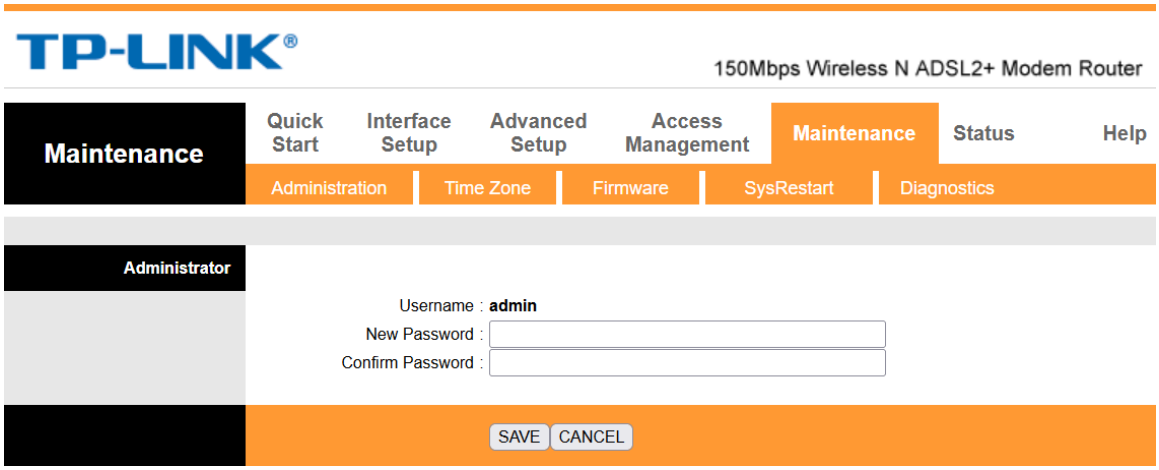


- ستظهر لك صفحة تسجيل الدخول الى اعدادات الراوتر وهنا نبين اول عملية تحقق من بيانات الهوية من اجل الدخول للراوتر(Authentication) والتي كما ذكرنا سابقا ان هذه البيانات افتراضية معروفة في العادة للجميع. لذا سنغيرها لاحقا الى بيانات هوية خاصة بك لا احد يعلمها الا انت.
الان قم بكتابة اسم المستخدم Username = admin حروف صغيرة. وقم بكتابة **كلمة المرور** التى تجدها على ظهر الراوتر Password سواء حروف صغيرة أو كبيرة كما هي

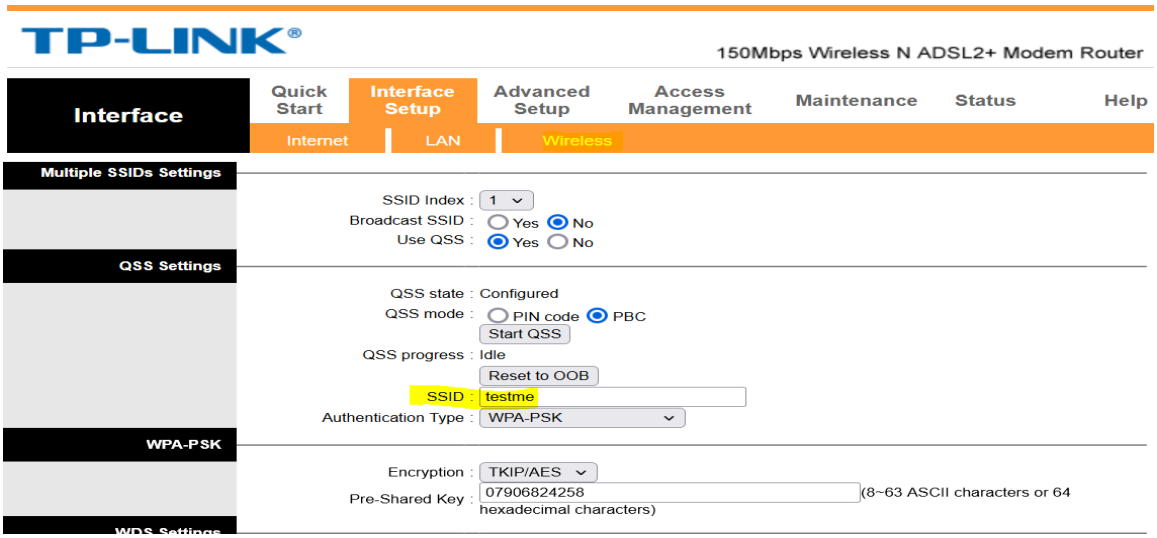
- بعد كتابة admin و كلمة السر المكتوبة في ظهر الراوتر كما هو موضح بالأعلي سندخل علي صفحة الإعدادات



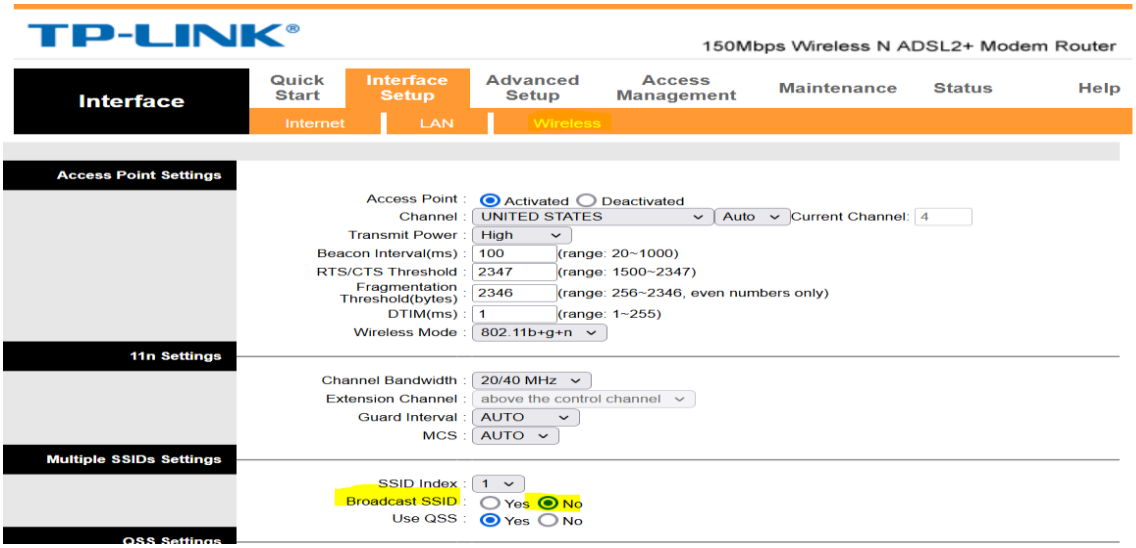
- يمكنك تغيير كلمة المرور اللازمة للدخول الى الراوتر(بدلا من كلمة المرورالافتراضية التي تكون غالبا من الشركة هي admin) كما في الشكل ادناه:



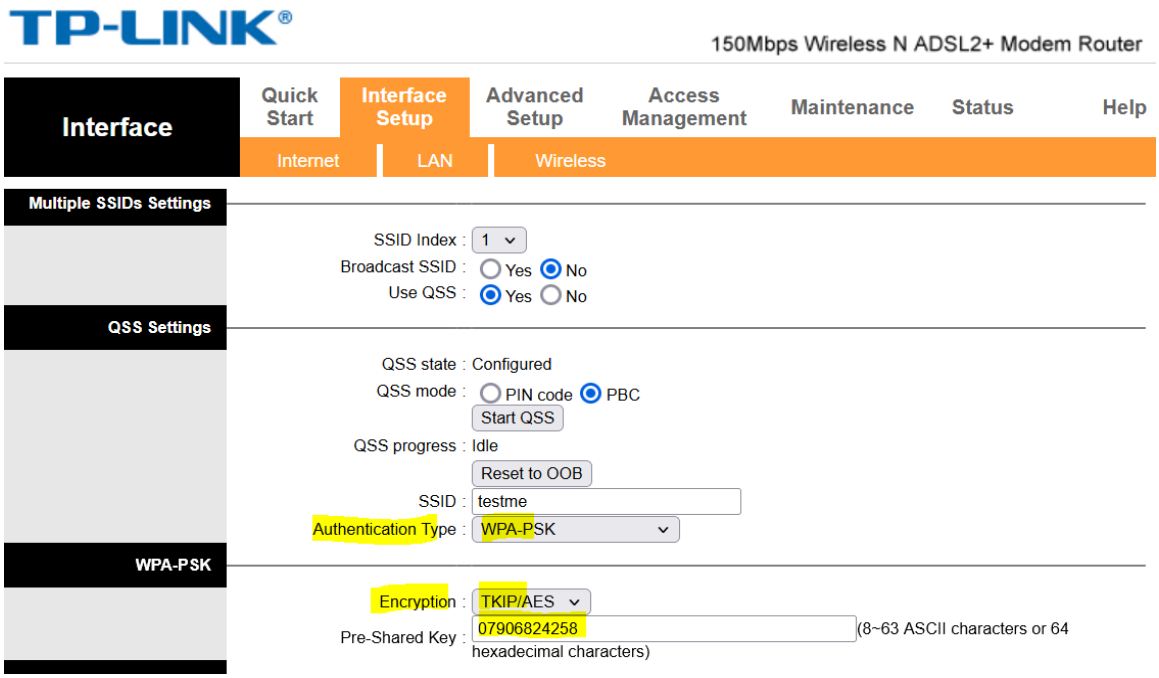
- يمكنك تغيير الاسم الافتراضي الخاص بالشبكة اللاسلكية(SSID) والذي يكون عادة نفس اسم الراوتر الى الاسم الذي تريد كما في الشكل ادناه:



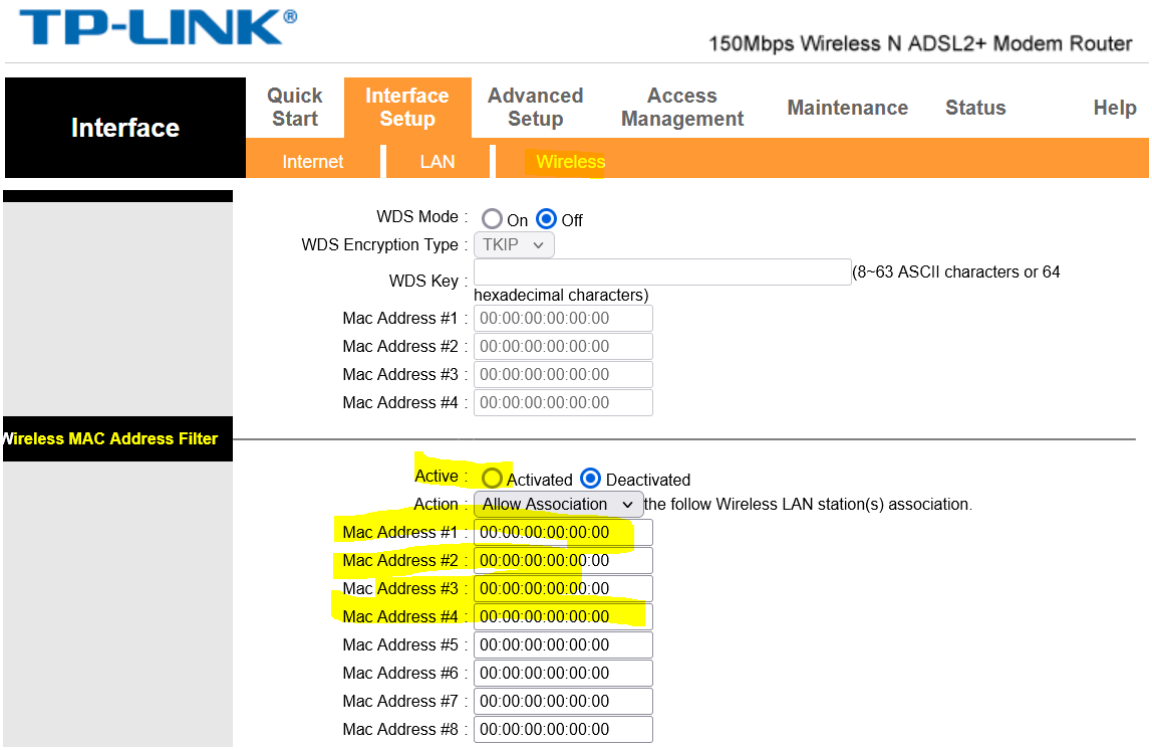
- يمكنك اخفاء الشبكة اللاسلكية الخاصة بك عن العموم. فلا تظهر امام العموم عند البحث بالشكل التقليدي عن الشبكات اللاسلكية في حين يمكنك تمكين فقط من تريد من الاتصال بها عن طريق اعطائه معرف الشبكة SSID وذلك من خلال تعطيل خاصية SSID Bradcasting كما في الشكل ادناه:



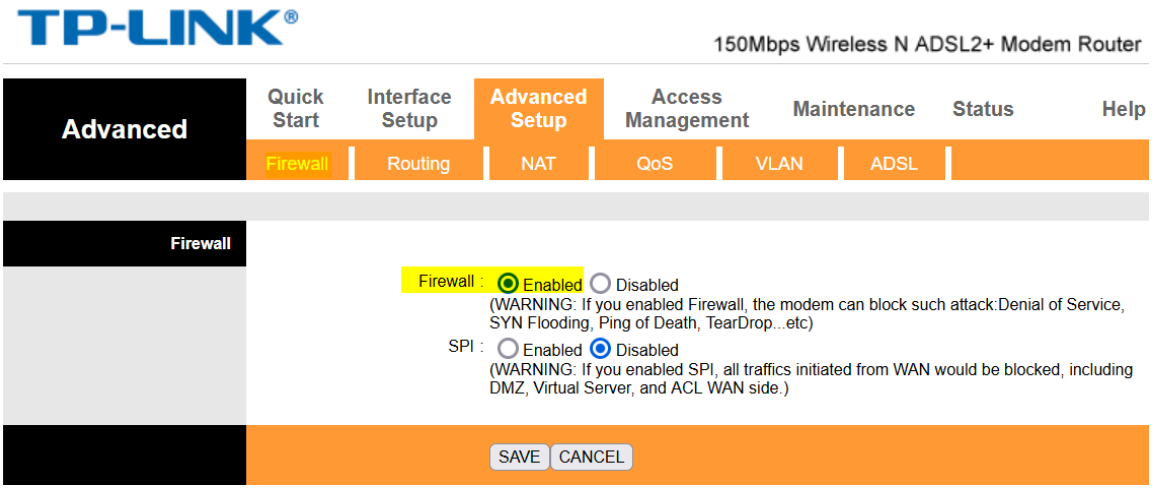
- يمكنك وضع كلمة مرور ملزم معرفتها لكل من يريد الاتصال بالشبكة اللاسلكية من خلال خاصية WPA و خاصية TKIP واللتين تستخدما لتحقيق مفهومي السرية (تشفير البيانات المتناقلة) و المصادقة (التحقق من هوية الجهاز المتصل) كما في الشكل ادناه:



- يمكنك تطبيق فلترة لعناوين MAC التي يقبل الاتصال بالشبكة اللاسلكية منها ويرفض من غيرها,فكما ذكرنا سابقا انه يمكن انشاء قائمة بعناوين MAC للاجهزة التي يسمح لها الاتصال بالشبكة وبالتالي يتم رفض اي اتصال قادم او اي محاولة اتصال من جهاز يملك عنوان MAC غير مدرج في القائمة كما في الشكل ادناه:



- يمكنك تفعيل خاصية الجدار الناري (Firewall) على جهاز الراوتر والذي يفيد في حماية الشبكة اللاسلكية من بعض انواع الهجمات المعروفة مثل SYN Floodong, DOS …… كما في الشكل ادناه:



الجلسة العملية الثانية

Packet Sniffing and Flooding Attack Penetration Test

(تشمم حركة حزم البيانات لتحقيق هجوم منع الوصول للشبكة اللاسلكية)

وصف الجلسة:

اغلب الهجمات التي يتم تفيذها ضد الشبكات اللاسلكية يحتاج فيها المهاجم الى التنصت على حزم البيانات المنتقلة داخل الشبكة ومن ثم الاستفادة من الكثير من البيانات المهمة التي تحتويها تلك الحزم. تختلف النظرة الى محتويات الحزم من مهاجم الى اخر تبعا الى نوعية وطبيعة الهجوم الذي يسعى فيه المهاجم الى تنفيذه ضد الشبكة اللاسلكية هناك الكثير من الادوات و البرمجيات التي تمكن من تتبع محوتيات حزم البيانات في الشبكات اللاسلكية. في هذه الجلسة سيتم مراقبة حزم البيانات المتبادلة بين الاجهزة من جهة و AP من جهة اخرى ومن ثم استنباط المحتوى اللازم لتفيذ هجوم اغراق الجهاز المتصل بالحزم لتعطيل اتاحة الشبكة اللاسلكية امامه. وتذكر عزيزي الدارس ان الغرض من تطبيق الجلسة هو اختبار الاختراق اي التعرف على اساليب تنفيذ مثل تلك الاختراقات والهجمات لتجنبها والحماية منها وليس لشنها.

اهداف الجلسة

- تطبيق خطوات اضافة كرت الشبكة اللاسلكي الخارجي وتهيئته لتمكين تتبع الحزم .
- تطبيق الاوامر اللازمة للتعامل مع مشاكل عمل كرت الشبكة الخارجي.
- تطبيق اوامر تحويل اوضاع كرت الشبكة الخارجي.
- تطبيق اوامر عرض الشبكات اللاسلكية المحيطة بك وبياناتها المعرفة لها مثل MAC و ESSID وغيرها.
- تطبيق اوامر عرض الاجهزة المتصلة بشبكة مختارة على قناة معينة وبياناتها المعرفة لها مثل MAC.
- تطبيق اوامر تتبع وتشمم حزم البيانات (Packet Sniffing) المتبادلة بين جهاز ما و AP في الشبكة.
- تطبيق اوامر اغراق AP لشبكة لاسلكية بطوفان من حزم البيانات.
- تطبيق عرض نتيجة اغراق الشبكة وتعطيلها.

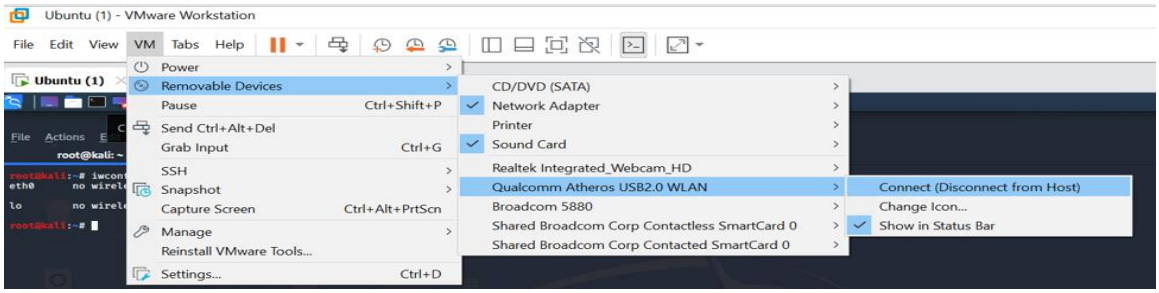
نظام التشغيل المستخدم في تطبيق الجلسة:

Kali Linux

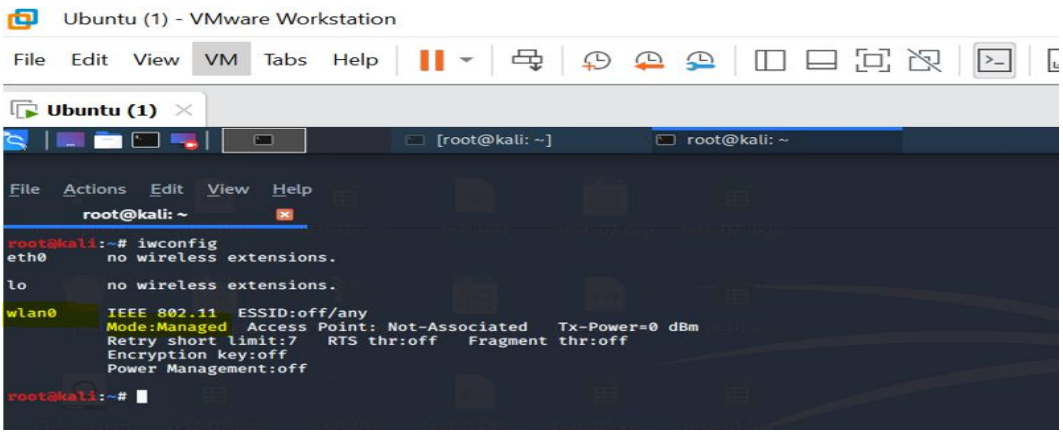
تطبيق الجلسة:

- يمكنك ان تقوم بتنزيل نظام التشغيل kali linux على احدى برمجيات الاجهزة الافتراضية مثل VMware لتجعله نظام تشغيل تخيلي وليس حقيقي. علما انه بامكانك تنزيل نظام kali linux بشكل حقيقي على جهازك فيصبح جهازك يحوي على نظامي تشغيل الويندوز والكالي. تم اعتماد Kali Linux المثبت على برمجية VMware في هذه الجلسة
- تحتاج الى كرت شبكة لاسلكي خارجي ووصله من خلال احد منافذ USB في جهازك. السبب من استخدام كرت خارجي هو الحاجة لتحويل حالته من Managed Mode الى Monitor Mode لتنفيذ الخطوات اللاحقة حيث ان اغلب البطاقات اللاسلكية الداخلية في اجهزة اللابتوب لا تدعم عملية التحول الى Monitor Mode

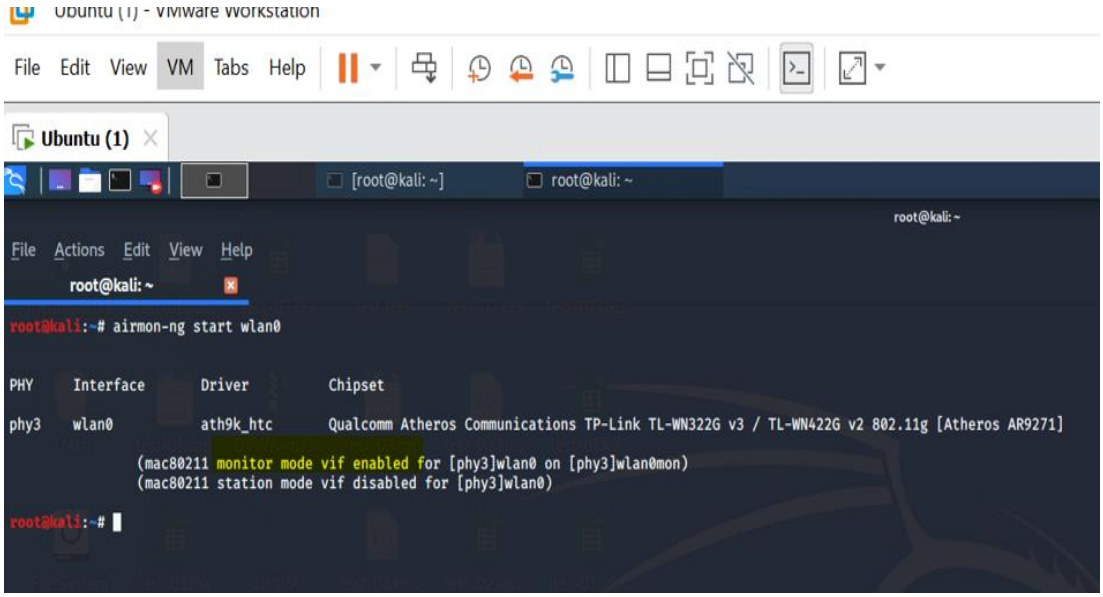
- بعد ان تقوم بوصل كرت wireless usb في مدخل usb بجهازك تاكد من ان VMware للكالي متعرفة على هذا الكرت وانها connected كما في الشكل(تذكر ان اغلب كروت الشبكة اللاسلكية الداخلية للابتوب لا تدعم تنفيذ الاوامر القادمة لاختبار الاختراق)



- يفترض الان ان كرت ال wireless الخارجي موصول نبدا بالخطوات:
افتح اي نافذة اوامر في النظام (terminal) لتنفيذ الاوامر القادمة:
  - **iwconfig** وهو الامر الذي يبين ان كان الجهاز فعلا تعرف على كرت wireless الجديد المضاف حيث سيظهر اسمه بالعادة باسم wlan0 لكن ان لم يظهر رغم اننا اضفناه بشكل صحيح فهذا قد يعني انه فعلا تم اضافته لكنه غير مفعل فنستخدم الامر
  - **Ifconfig wlan0 up** ثم نفحص مرة اخرى من خلال الامر iwconfig فسنراه لكن سنراه في وضع managed

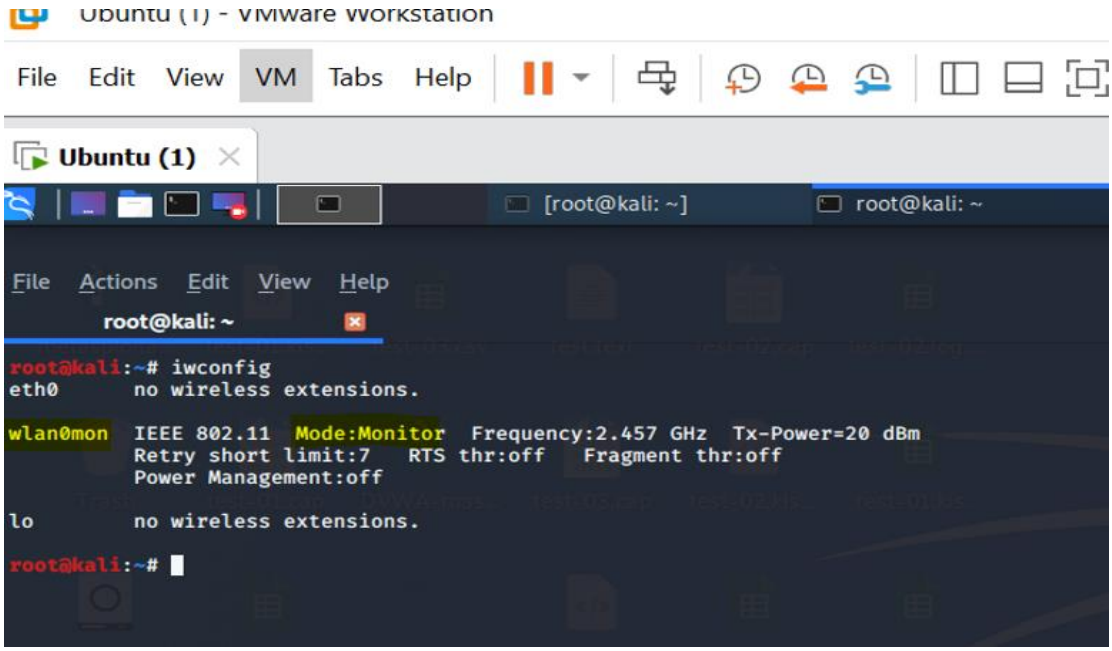


- نحول وضعه الى monitor وذلك من خلال الامر **airmon-ng start wlan0**



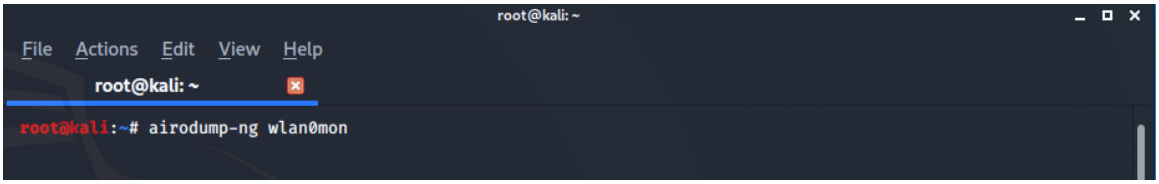
اذا لم تنجح عملية التحويل الى Monitor فهذا يعني ان هناك عمليات بحاجة الى توقيف ويتم ذلك من خلال الامر **kill check airmon-ng ثم نعيد تنفيذ امر التحويل السابق مرة اخرى**

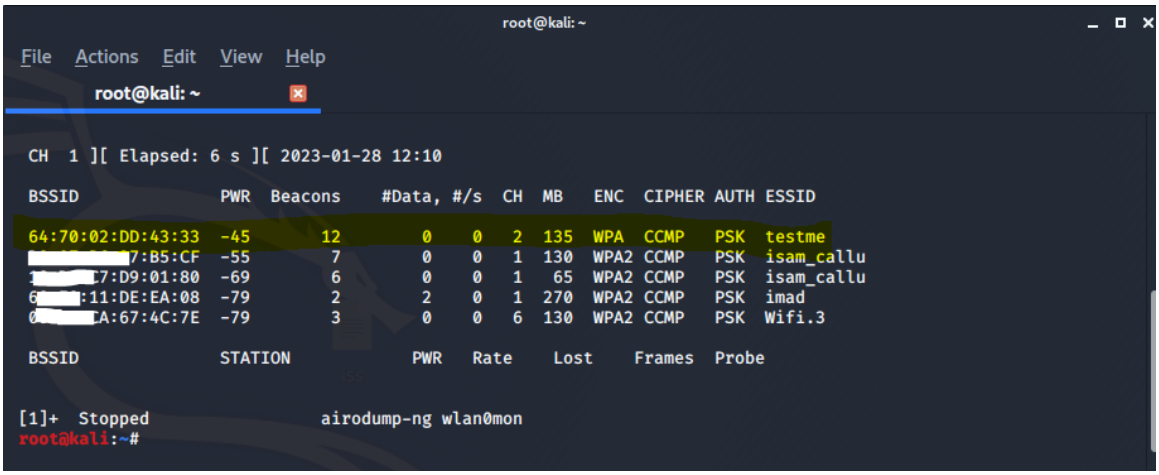
- الان نفذ الامر **iwconfig** لن يظهر لك كرت باسم wlan0 انما اصبح اسمه wlan0mon



- نريد عرض كل access points التي يستطيع كرت الشبكة الخاص بجهازنا التقاطها الامر هو

airodump-ng wlan0mon ستظهر لك قائمة بالشبكات وتفاصيلها مثل mac و channels و ESSID و BSSID وغيرها.....

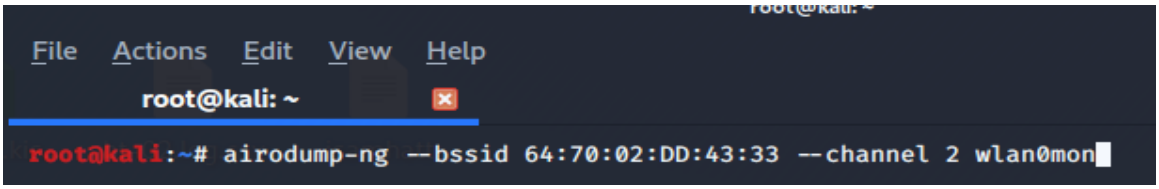


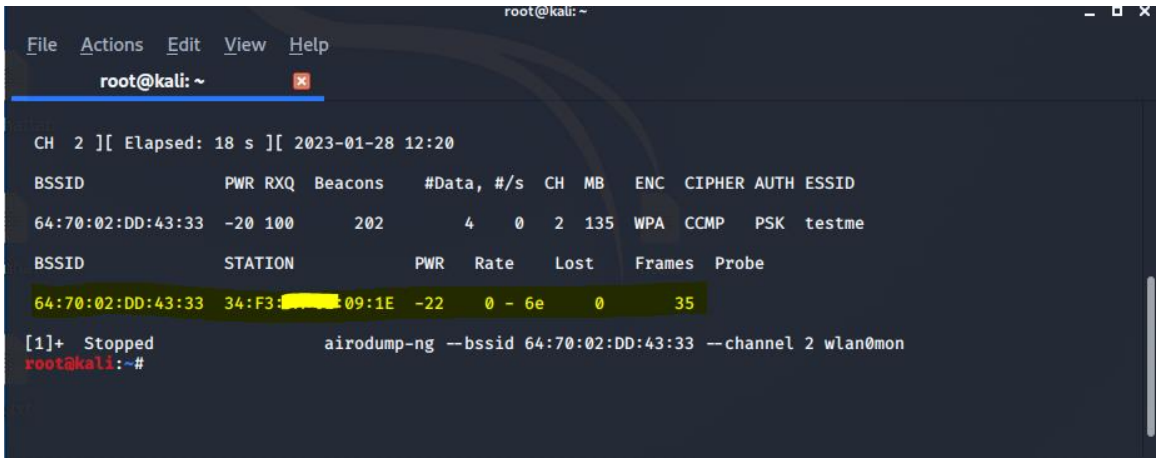


نضغط من لوحة المفاتيح CTRL+Z للتوقف عن عرض المزيد من الشبكات

- الان نريد اختيار access point ما لتتبعها وسنختار AP الخاصة بنا والتي نريد تتبع حزم البيانات الذاهبة اليها والقادمة منها الامر هو

airodump-ng --bssid رقم الماك الخاص بهذه الاكسس بوينت التي نريد --channel رقم القناة الخاص بالاكسس بوينت التي نريدها wlan0mon



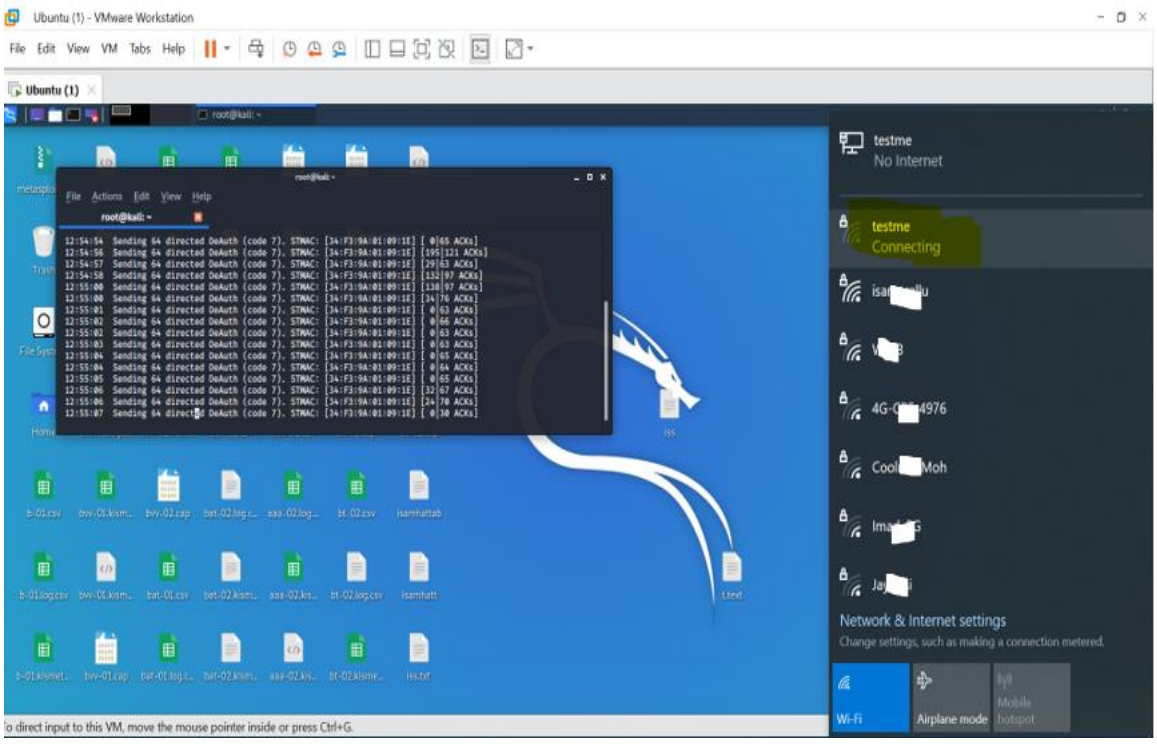


نلاحظ في الشاشة اعلاه ان الجهاز الوحيد المتصل على هذه الشبكة (Essid:testme) هو الجهاز المشار اليه في اللون الاصفر وايضا استطعنا معرفة MAC Address الخاص به

- الان نريد فصل الجهاز الذي نعمل علية والمتصل اصلا بهذه الاكسسبوينت من الاتصال

aireplay-ng -0 عدد الحزم المرسلة -a رقم الماك للاكسسبوينت --c رقم الماك لهذا الجهاز wlan0mon

يعني هذا الامر اننا سنقوم باغراق هذا الجهاز (المحدد بالماك ادرس المبين والمتصل بالشبكة) باعداد من 600 من حزم الطلب وبالتالي سيؤدي الى ان يبقى هذا الجهاز فاقدا للاتصال كما هو موضح بالشكل ادناه :



ولايقاف هجوم هذا الطوفان من الحزم على الجهاز ننهي الامر بالضغط على CTRL+Z

الجلسة العملية الثالثة

MAC Address Spoofing Penetration Test

(انتحال عنوان MAC لجهاز متصل في الشبكة)

وصف الجلسة:

من الاستراتيجيات الامنية التي تطبيق في الشبكات اللاسلكية لحمياتها من الدخلاء هي عمل فلترة لعناوين MAC للاجهزة التي يسمح لها بالاتصال بالشبكة. بمعنى تحديد قائمة بعناوين MAC الاجهزة التي تقبل AP الاتصال بها ورفض الاتصال من اي عنوان عدا ذلك (غير موجود في القائمة). في هذه الجلسة سيتم عمل تتبع لعناوين الاجهزة المتصلة بالشبكة (بالتالي فهي تملك MAC مسموح الاتصال منه) ومن ثم تغيير عنوان كرت الشبكة الخارجي (MAC) الذي نعمل من خلاله الى عنوان MAC احد الاجهزة المتصلة ليتم قبول جهازنا والتمكن من الاتصال بالشبكة (انتحال عنوان MAC لجهاز متصل). وتذكر عزيزي الدارس ان الغرض من تطبيق الجلسة هو اختبار الاختراق اي التعرف على اساليب تنفيذ مثل تلك الاختراقات لتجنبها والحماية منها وليس لشنها

اهداف الجلسة

- تطبيق اوامر تبديل اوضاع كرت الشبكة الخارجي .
- تطبيق اوامر التعرف على عناوين MAC الخاص بكرت الشبكة.
- تطبيق اوامر عرض الشبكات اللاسلكية وعناوينها MAC.
- تطبيق اوامر عرض عناوين MAC للاجهزة المتصلة مع AP في الشبكة اللاسلكية.
- تطبيق اوامر تغيير عنوان MAC الخاص ببطاقة الشبكة الخارجي الى عنوان اخر.

نظام التشغيل المستخدم في تطبيق الجلسة:

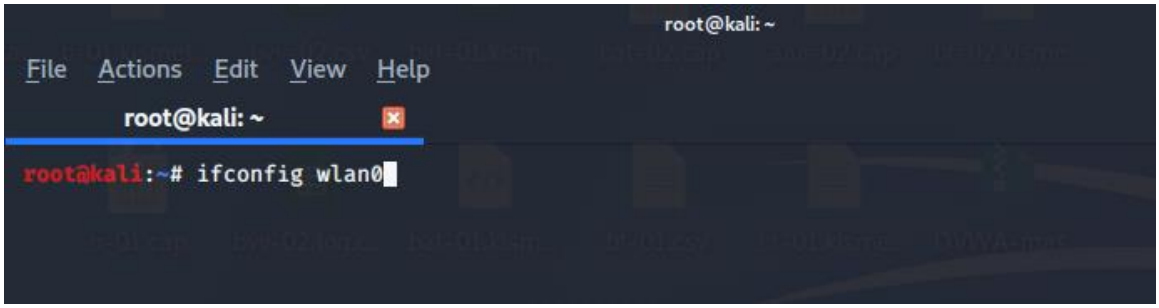
Kali Linux

تطبيق الجلسة:

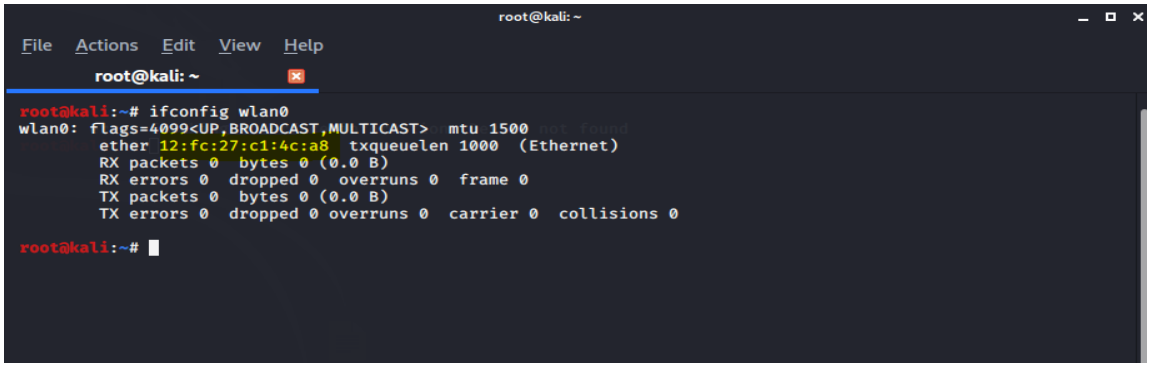
- تباعا للجلسة العملية السابقة فان كرت الشبكة اللاسلكي الخارجي مازال في حالة Monitor Mode.سنقوم بارجاعه الى حالته الافتراضية وهي Managed Mode من خلال الامر المبين في الشكل ادناه:

- وللتاكد من ذلك (انه Managed Mode) فان الامر الذي مر معنا في الجلسة السابقة iwconfig يبين لنا انه فعلا اصبح في Managed Mode وانه تغير اسمه من wlanomon الى wlan0 كما في الشكل:

- سنستخدم الامر المبين في الشكل ادناه لمعرفة عنوان MAC الخاص بكرت الشبكة اللاسلكية الحالي(الخارجي الذي نعمل عليه):

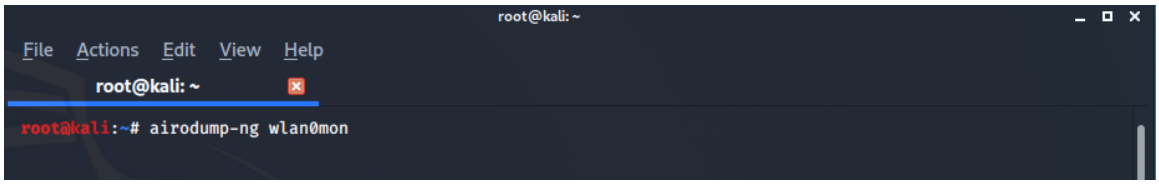


- ليظهر كما في الشكل ادناه:

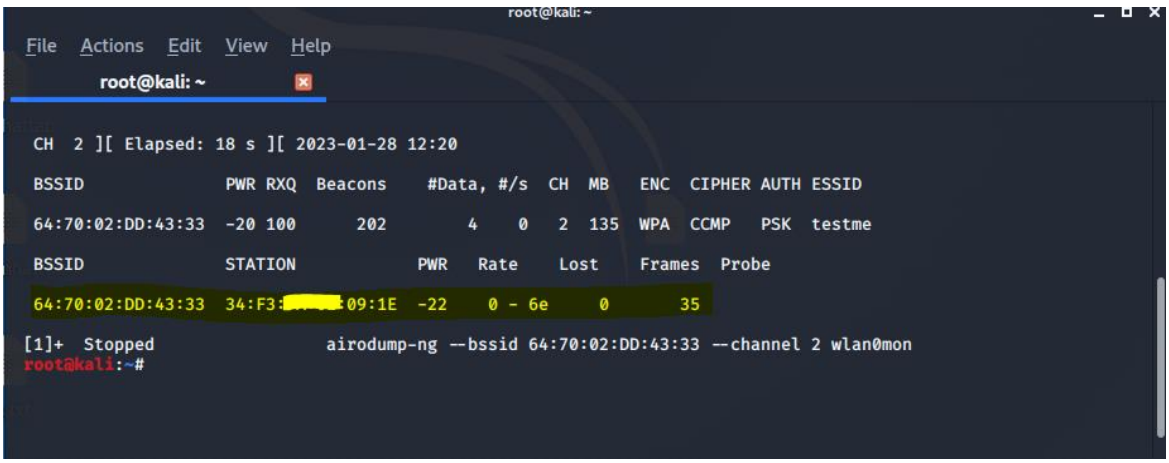


- الان سنقوم باعادة تحويله الى Monitor Mode من خلال الامر المبين في الشكل ادناه:

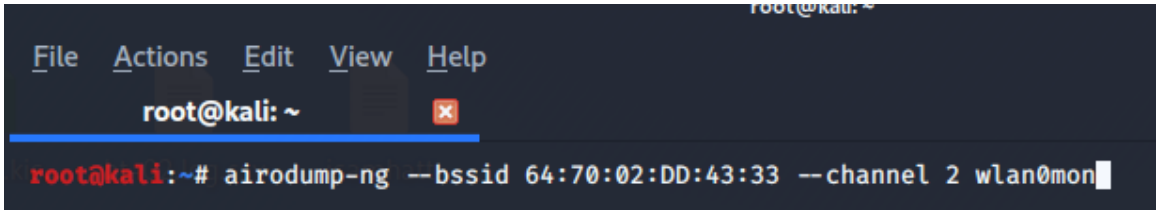
- سنقوم بعرض كل access points التي يستطيع كرت الشبكة الخاص بجهازنا التقاطها من خلال الامر الموضح في الشكل ادناه كما مر سابقا :

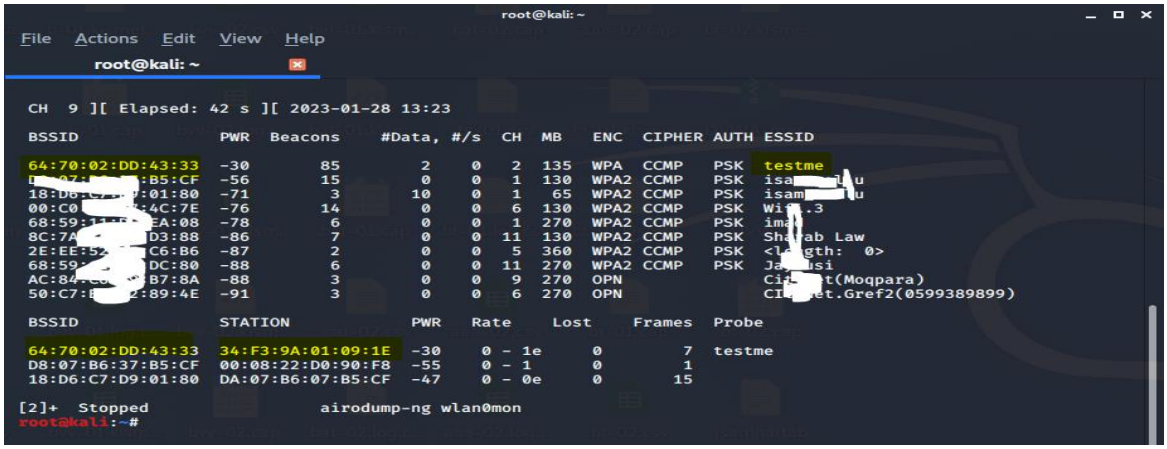


- لتظهر فعلا الشبكات اللاسلكية وتفاصيلها كما هو مبين ادناه:

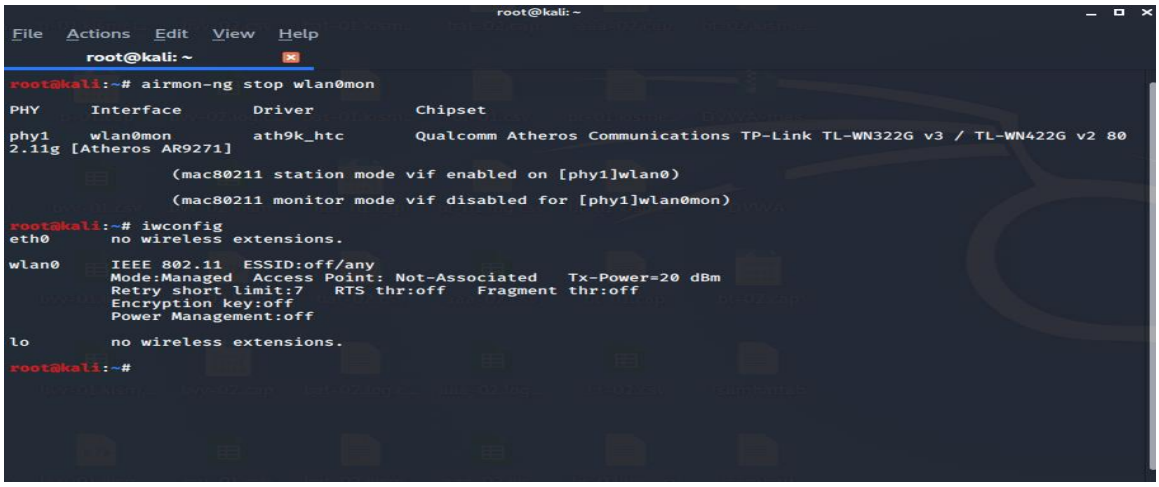


- الان نريد اختيار access point ما لتتبعها وسنختار AP الخاصة بنا وسنكتشف عناوين MAC المتصلة بها بنجاح (العناوين المقبولة حسب الفلترة) من خلال الامر المبين:

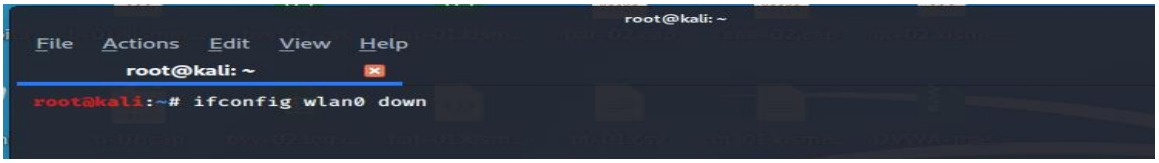




- سنبدا بخطوات تغيير عنوان MAC الخاص بكرت شبكتنا الخارجي الى عنوان MAC ذلك الجهاز المتصل بالشبكة (المظلل باللون الاصفر) حيث سنبدا بامر ايقاف Monitor Mode وارجاعه الى Managed Mode والتاكد من اتمام التحول بنجاح من خلال الاوامر التي مرت في بداية هذه الجلسة والموضحة في الشكل ادناه:

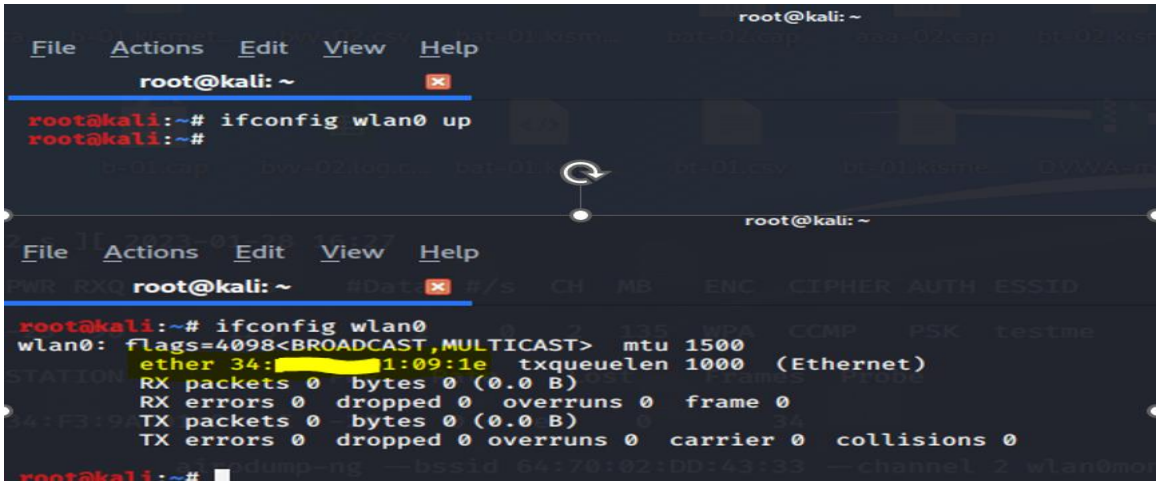


- سنوقف عمل بطاقة الشبكة مؤقتا من خلال الامر التالي المبين:

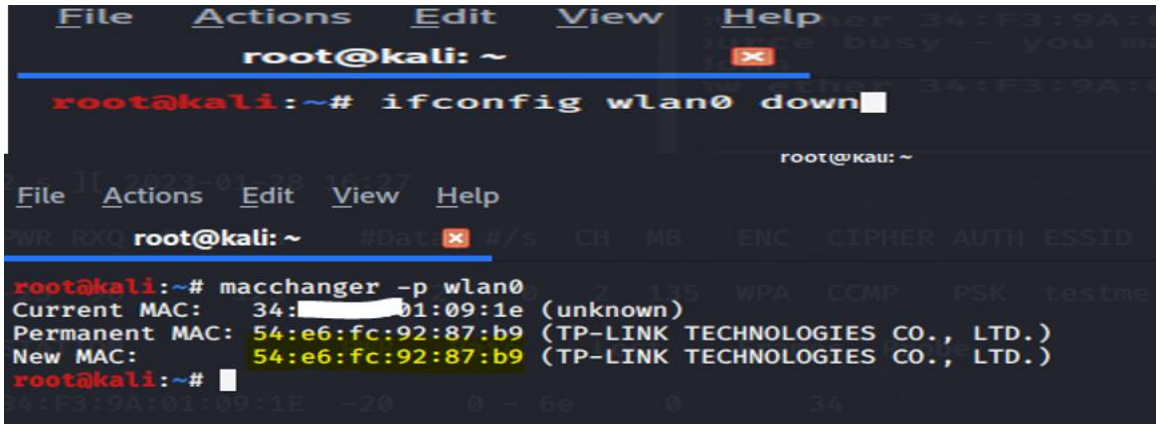


- سننفذ امر تغيير عنوان MAC الخاص ببطاقة الشبكة بنا الى عنوان MAC للجهاز المتصل كما في الشكل ادناه:

- اخيرا من اجل التاكد ان بطاقة الشبكة قد تغير MAC الخاص بها فعليا فاننا نتبع الاوامر في الصورة ادناه:



- الان اصبح كرت الشبكة الخاص بنا يملك عنوان MAC منتحل لعنوان MAC مقبول ويمكنه الاتصال بالشبكة اللاسلكية.
- في حال ان جهازك الحقيقي (المثبت عليه Windows) صاحب عنوان MAC السابق اصبح غير قادر على الاتصال في شبكتك اللاسلكية فانك بحاجة الى اعادة تغيير عنوان MAC الخاص بالبطاقة الخارجية الى عنوانها الاصلي من خلال الاوامر المبينة في الشكل ادناه:



- ومن ثم نعيد تشغيل الويندوز

الجلسة العملية الرابعة

Deauthentication Attack Penetration Test

(هجوم المصادقة لاكتشاف الشبكات المخفية(Disabled ESSID Broadcasting))

وصف الجلسة:

من الاستراتيجيات الامنية التي تطبق في الشبكات اللاسلكية لحمياتها من الدخلاء هي اخفاء بيانات معرف الشبكة اللاسلكية عن الاجهزة (ESSID Broadcasting off) كما مرمعنا في الجلسة الاولى.فمن المعلوم ان الجهاز يقوم بعمل مسح لاكتشاف الشبكات اللاسكية المحيطة به ومن ثم يحدد واحدة منها ليقوم بالاتصال بها. ومن الاجراءات الامنية الاضافية التي يمكن اتباعها كما تم توضيحه ان يتم اخفاء اسماء نقاط العبور للشبكة اللاسلكية(ESSID Broadcasting) وبالتالي لا تظهر للغريب في حين يستطيع الجهاز فقط الذي يعلم هذا المعرف مسبقا الاتصال بها.في هذه الجلسة سيتم التعرف على احدى الطرق التي يستخدمها المهاجم ويوظفها لاكتشاف الشبكات اللاسلكية المخفية عنه من خلال استغلال هجوم يشنه على الشبكة يدعى (Deauthentication Attack) والذي يستخدمه لفصل اتصال جهاز ما في الشبكة اللاسلكية واعادة اتصاله معها مرة اخرى بعد ان يقدم بيانات الممصادقة ل AP والتي يستفيد منها المهاجم لاكتشاف ESSID الخاص بالشبكة. تذكر عزيزي الدارس ان الغرض من تطبيق الجلسة هو اختبار الاختراق اي التعرف على اساليب تنفيذ مثل تلك الاختراقات لتجنبها والحماية منها وليس لشنها

اهداف الجلسة

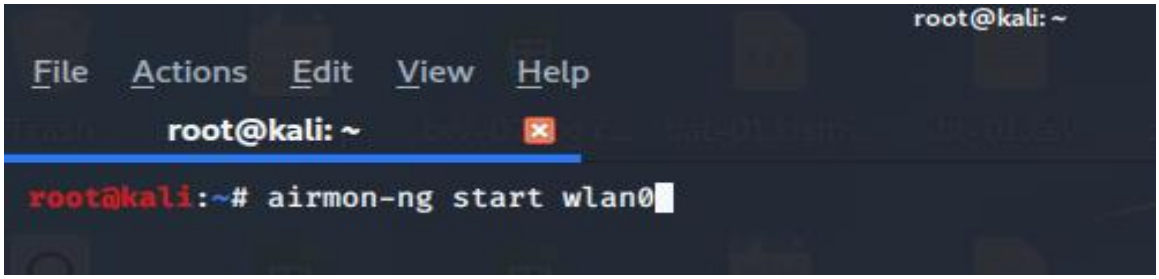
- تطبيق اوامر عرض الشبكات اللاسلكية المحيطة بك وبياناتها المعرفة لها مثل MAC و ESSID وغيرها.
- التعرف على الشبكات اللاسلكية المخفية.
- تطبيق اوامر عرض الاجهزة المتصلة بشبكة مختارة مخفيةعلى قناة معينة وبياناتها المعرفة لها مثل MAC.
- تطبيق اوامر تنفيذ Deauthentication لجهاز محدد لفصل اتصاله من الشبكة.
- تطبيق اظهار الشبكة المخفية.

نظام التشغيل المستخدم في تطبيق الجلسة:

Kali Linux

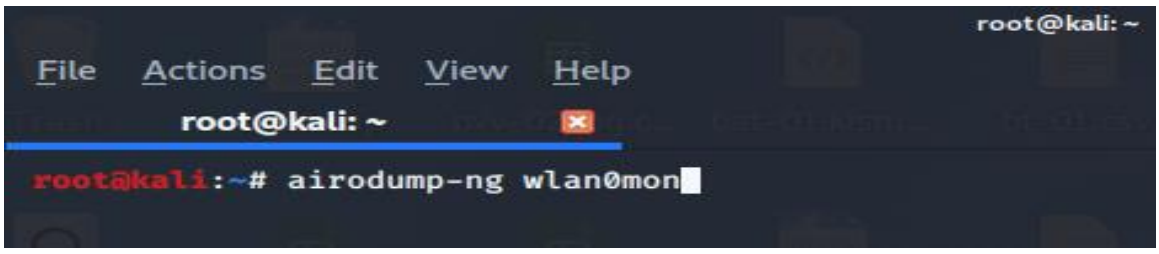
تطبيق الجلسة:

- اعتمادا على تطبيق عملية الاخفاء للشبكة اللاسلكية في الجلسة الاولى فان الشبكة اللاسلكية يفترض انها مخفية.
- نقوم بتغييروضعية كرت الشبكة الخارجي الى Monitor Mode بنفس الطريقة التي مرت في الجلسات السابقة وكما هو موضح ادناه:

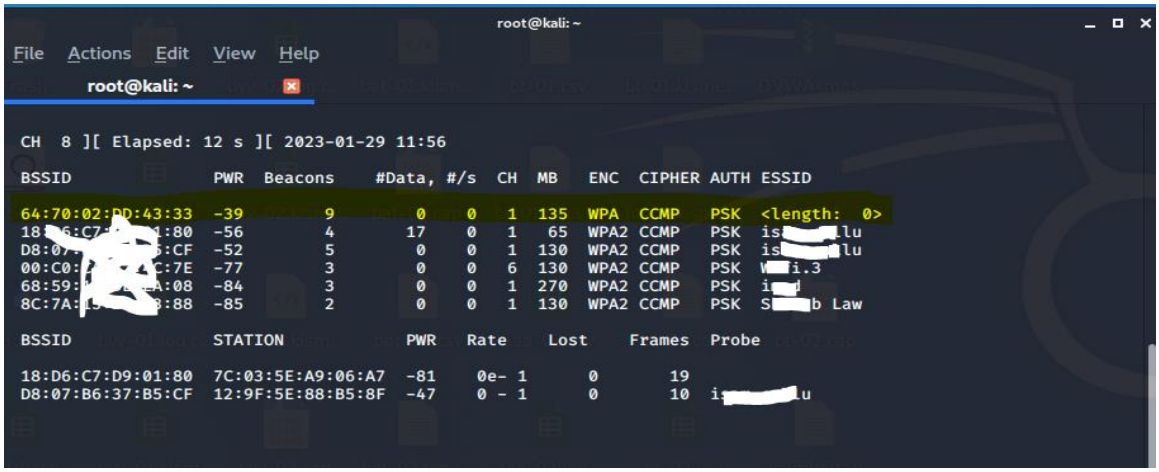


- للتاكد من ان الكرت اصبح بالفعل بوضح Monitor Mode نستخدم الامر iwconfig

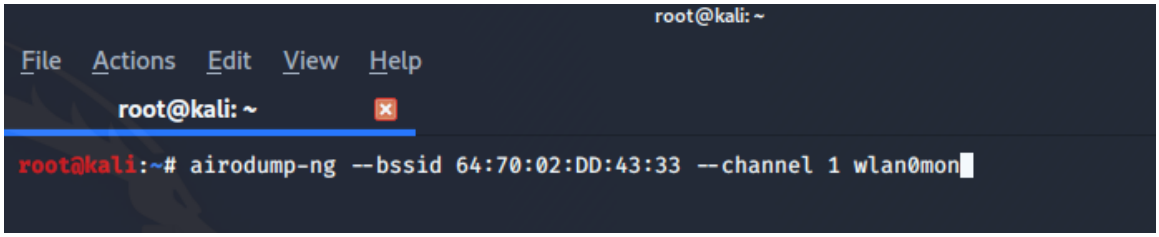
- سنقوم بعرض كل access points التي يستطيع كرت الشبكة الخاص بجهازنا التقاطها من خلال الامر الموضح في الشكل ادناه كما مر سابقا :



- لتظهر فعلا الشبكات اللاسلكية وتفاصيلها وبان احدى هذه الشبكات ESSID لها هو length: 0 والذي يدل ان هذه الشبكة مخفية (ESSID Broadcasting is disabled) كما هو مبين ادناه:



- الان سنقوم بالنتصت (Sniffing) على هذه الشبكة باستخدام بيانات رقم MAC الخاص بها و رقم القناة ومن خلال الامر الذي مر معنا سابقا كما هو مبين ادناه:

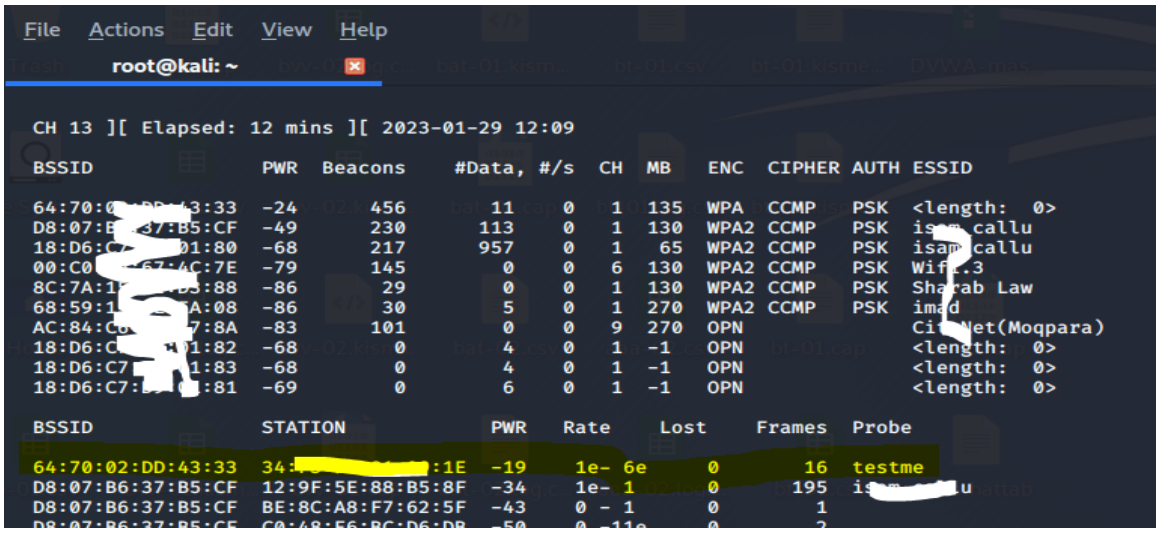


- النتيجة هي انه يوجد جهاز على الاقل متصل بها (وهو جهازنا الحقيقي(windows) في هذه التجربة) ويظهر عنوان MAC الخاص به كما هو :

- الان نحن بحاجة الى التقاط عملية اتصال جديدة لجهاز مع الشبكة ليتم التقاط بيانات مصادقته مع الشبكة والاستفادة منها لاكتشاف ESSID الخاص بالشبكة. لذا بدلا من الانتظار طويلا لاتصال جديد مع احتمالية ان لا يتم اتصال جديد اصلا. سنقوم بقطع اتصال الجهاز المتصل(والذي حددنا عنوان MAC الخاص به بالخطوة السابقة) مع الشبكة واعادة اتصاله من جديد معها لالتقاط ESSID الخاص بها من خلال الاستفادة من بيانات اعادة المصادقة له مع الشبكة وهذا ما يسمى Deauthentication Attack من خلال الامر ادناه في شاشة اوامر جديدة (Terminal) مع الابقاء على شاشة استكشاف الشبكات اللاسلكية السابقة فعالة:

aireplay-ng -0 1 -a رقم الماك للاكسسبوينت --c رقم الماك لهذا الجهاز wlan0mon

- النتيجة هي انه سيظهر لنا ESSID للشبكة اللاسلكية المخفية كما هو موضح ادناه:



الجلسة العملية الخامسة

Dictionary Attack Penetration Test (اختبار اختراق كلمات المرور)

وصف الجلسة:

من المفاهيم الاساسية التي تستخدم لحماية الشبكات اللاسلكية هو حمايتها بكلمة مرور حتى تتمكن فقط الاجهزة المخولة التي تملك كلمة المرور هذه من الاتصال بالشبكة ورفض الاتصال القادم من الاجهزة عدا ذلك . في هذه الجلسة سيتم التعرف على احدى الطرق التي تستخدم من قبل المهاجمين لاكتشاف كلمات مرور الشبكات اللاسلكية وبالتالي استخدامها لتمكين اجهزتهم من الاتصال بالشبكة من خلال اليات تتبع الحزم وقراءة محتوياتها اللازمة لتحمين كلمة مرور الشبكة باستخدام برنامج Wireshark. تذكر عزيزي الدارس ان الغرض من تطبيق الجلسة هو اختبار الاختراق اي التعرف على اساليب تنفيذ مثل تلك الاختراقات لتجنبها والحماية منها وليس لشنها.

اهداف الجلسة

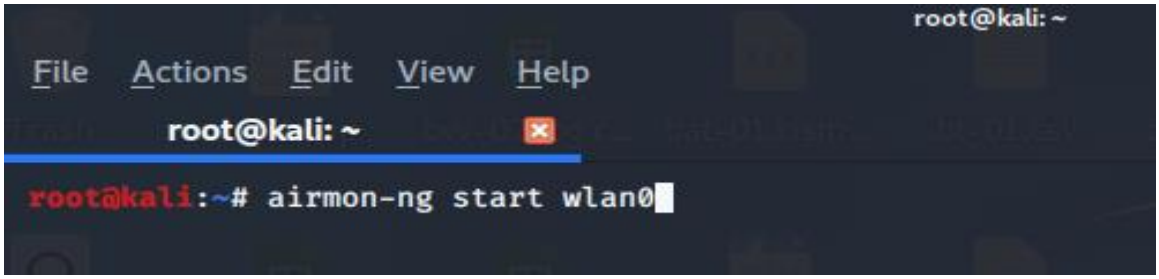
- تطبيق اوامر عرض الشبكات اللاسلكية المحيطة بك وبياناتها المعرفة لها مثل MAC و ESSID وغيرها.
- تطبيق اوامر عرض الاجهزة المتصلة بشبكة مختارة على قناة معينة وبياناتها المعرفة لها مثل MAC.
- تطبيق اوامر تتبع وتشمم حزم البيانات (Packet Sniffing) المتبادلة بين جهاز ما و AP في الشبكة.
- تطبيق اوامر التقاط حزمة المصادقة للجهاز مع الشبكة (Synk Packet).
- تطبيق اوامر الاحتفاظ بالحزم في ملف واستعراض محتوياتها من خلال برنامج Wireshark.
- تطبيق اوامر انشاء ملف بقائمة كلمات مرور مواصفات محددة (Password Dictionary).
- تطبيق اوامر هجوم القاموس (Dictionary Attack) لكسر كلمة مرور الشبكة.

نظام التشغيل المستخدم فى تطبيق الجلسة:

Kali Linux

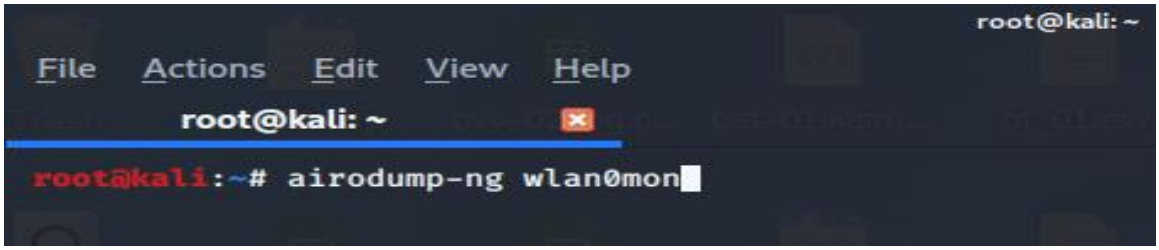
تطبيق الجلسة:

- نقوم بتغييروضعية كرت الشبكة الخارجي الى Monitor Mode بنفس الطريقة التي مرت في الجلسات السابقة وكما هو موضح ادناه:

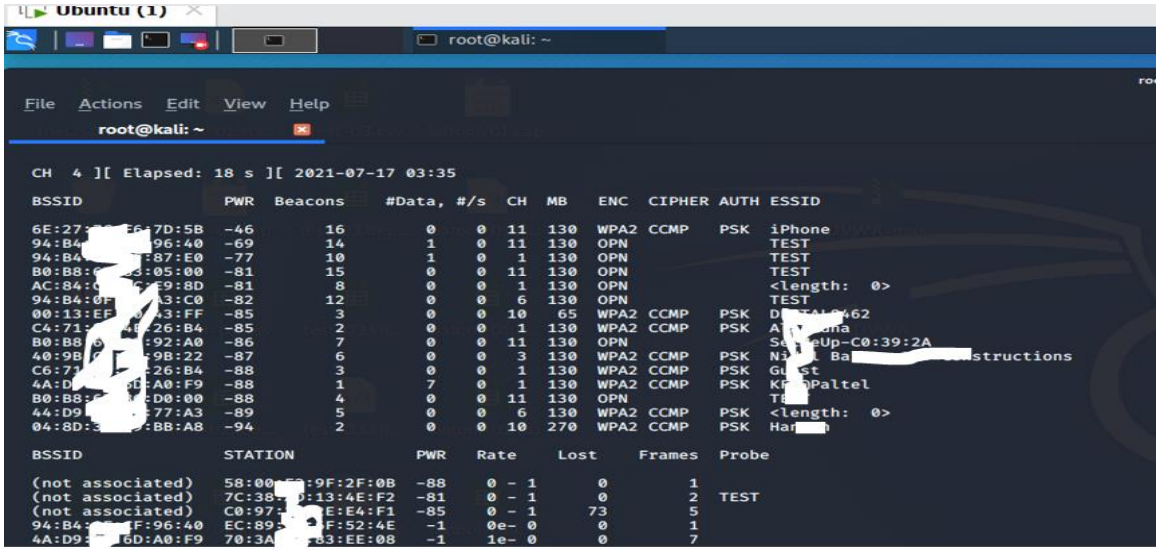


- للتاكد من ان الكرت اصبح بالفعل بوضح Monitor Mode نستخدم الامر iwconfig

- سنقوم بعرض كل access points التي يستطيع كرت الشبكة الخاص بجهازنا التقاطها من خلال الامر الموضح في الشكل ادناه كما مر سابقا :



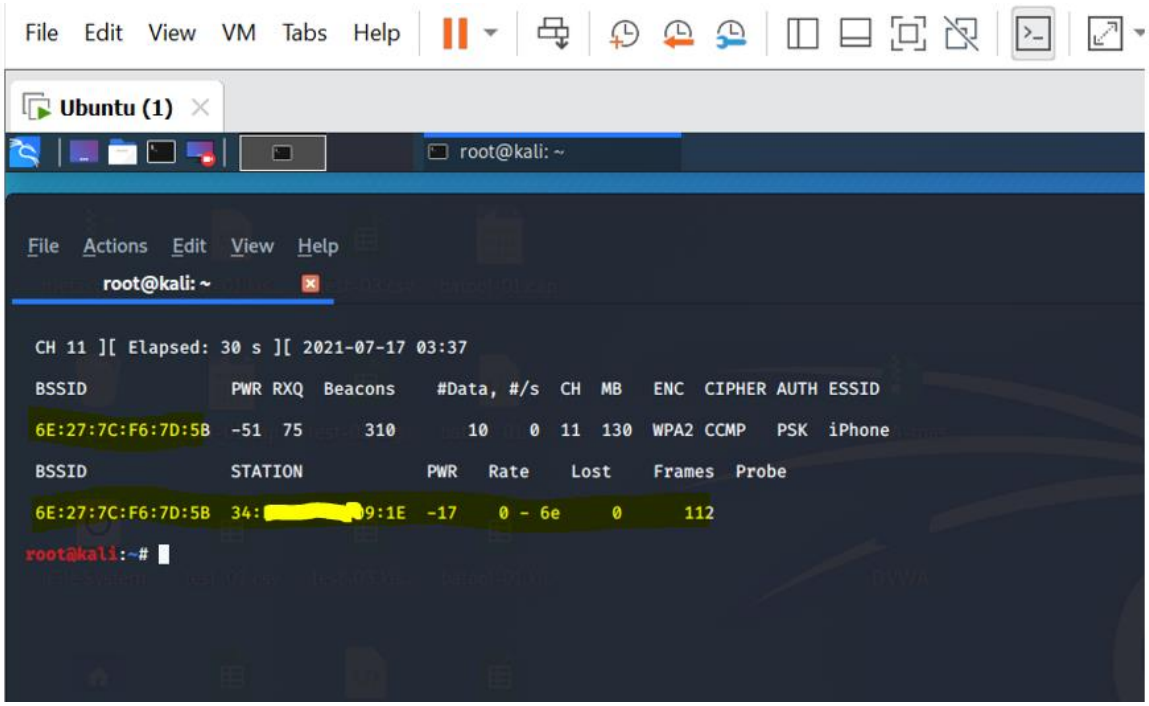
- لتظهر فعلا الشبكات اللاسلكية وتفاصيلها



- الان نريد اختيار access point الخاصة بنا والتي نريد تتبع حزم البيانات الذاهبة اليها والقادمة منها من خلال عنوان MAC الخاص بها من خلال الامر الذي مر معنا في الجلسات السابقة كما في الشكل:

```
root@kali:~# airodump-ng --bssid 6E:27:7C:F6:7D:5B  --channel 11  wlan0mon
```

- ناتج هذا الامر هو عرض الاجهزة المتصلة بهذه الشبكة وعلى رقم القناة المبينة (الجهاز الوحيد المتصل بهذه الشبكة هو جهازنا الحقيقي والمبين بالشكل ادناه من خلال عنوان MACالخاص به):



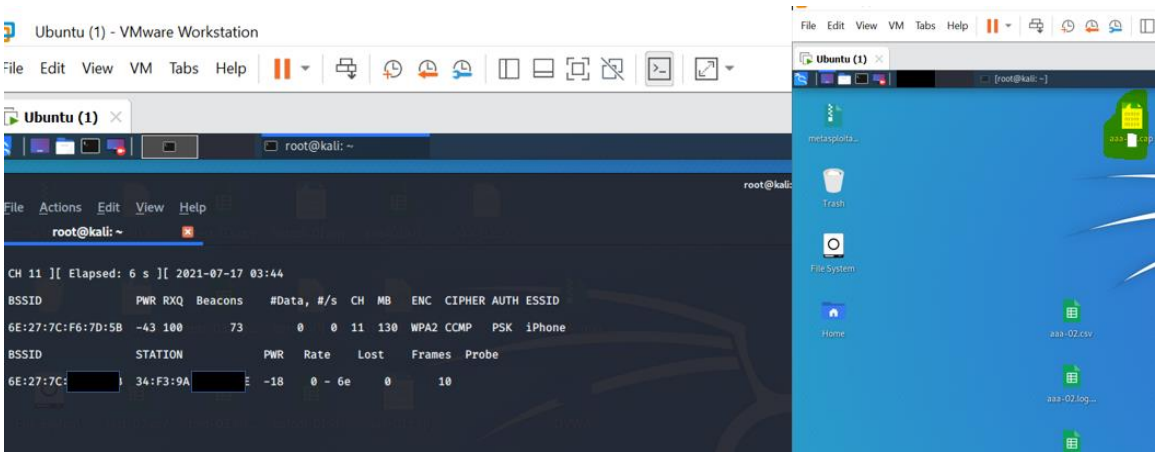
- الان نريد ان نحفظ تتبع الحزم السابق الذي تم بين الجهاز الخاص بنا والاكسسبوينت المتصل بها و هو نفس الامر الذي مر معنا في الجلسات السابقة لكن مع اضافة write–واسم الملف الذي نريد الحفظ فيه فيصبح الامر:

airodump-ng --bssid رقم الماك الخاص بهذه الاكسس بوينت التي نريد --channel رقم القناة
wlan0mon اسم الملف بمساره write-- الخاص بالاكسس بوينت التي نريدها

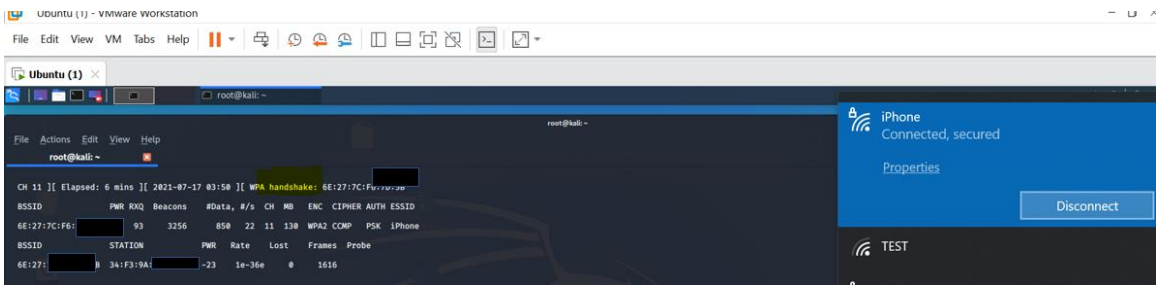
كما هو مبين ادناه:

```
root@kali:~# airodump-ng --bssid  6E:27:7C:F6:7D:5B --channel 11  --write Desktop/aaa wlan0mon
```

- ناتج الامر السابق عرض بيانات الجهاز المتصل بالشبكة وانشاء ملف على سطح المكتب باسم aaa يبقى يسجل ويحتفظ بكل الحزم المتبادلة بين الجهاز والشبكة كما هو مبين في الصور ادناه:



- فكما مر معنا في الجلسات السابقة نستخدم CTRL+Z لايقاف تتبع الحزم وانهاء تسجيلها بالملف.لكن لا فائدة من هذه الحزم اذا لم يكن احداها حزمة Handshaking Packet وهي حزمة المصافحة التي تحوي بيانات المصادقة بين الجهاز والشبكة. وكما نعلم ان المصادقة تتم عند بداية الاتصال من اجل قبوله اذا تمت بنجاح او رفضه. فاننا سنقوم بقطع اتصال الجهاز واتصاله من جديد مباشرة .عندما تظهر رسالة تفيد بان المصافحة تمت (كما في الشكل ادناه) فهذا يعني اننا استطعنا تسجيل حزمتها في الملف وبالتالي يمكننا الان انهاء التتبع للحزم من خلال CTRL+Z:



- الان نريد انشاء قائمة بكلمات المرور(قاموس لكلمات المرور) في ملف وذلك من خلال الامر :

Chrunch رقم يمثل الحد الادنى لخانات كلمة السر رقم يمثل الحد الاعلى لخانات كلمة السر
اسم الملف الذي تريد اشاؤه وحفظ قائمة كلمات السر هذه به -o خيارات كلمة السر
مثال:

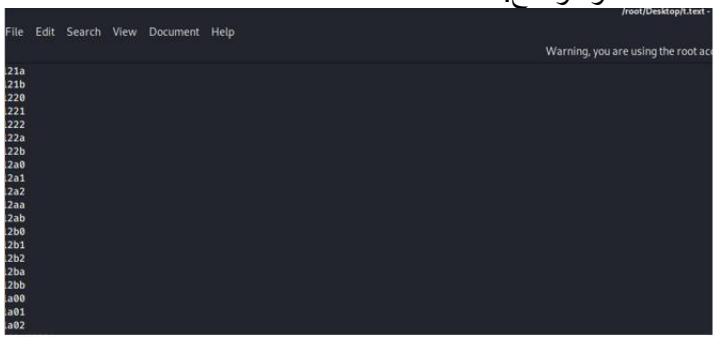
Chrunch 1 4 012ab -o Desktop/test.txt

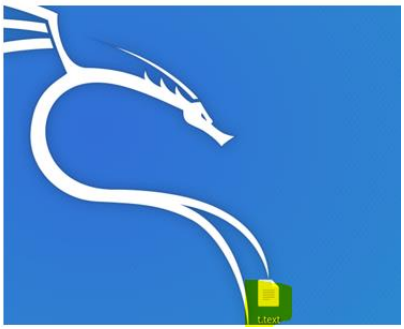
لو فتحنا هذه الملف سنرى عدد من كلمات السر مثلا

1
2
A
21
21a
Aaaa
Ba21

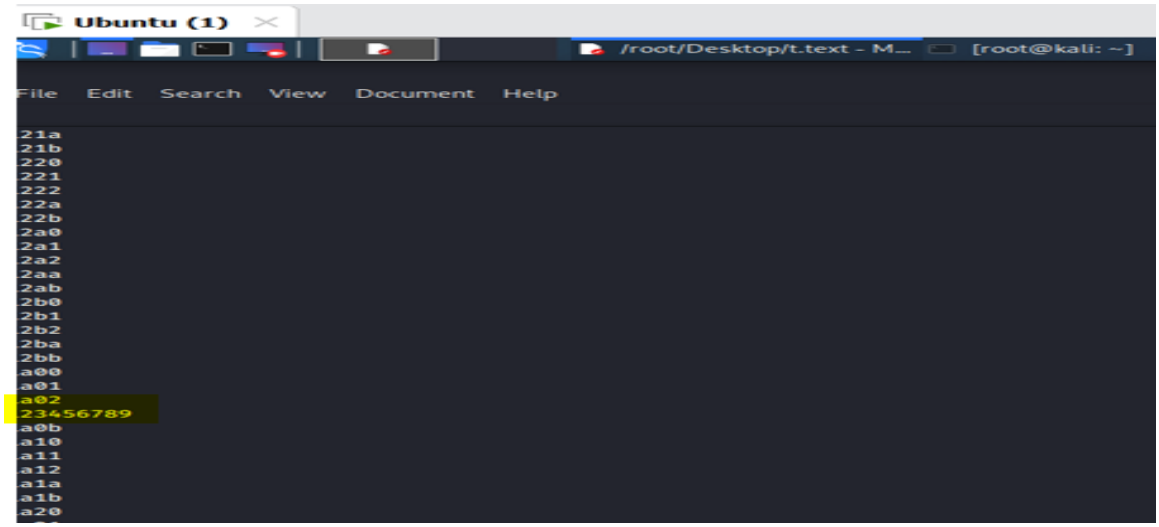
فلن نرى غير الخيارات ab012 ولن نرى كلمة سر عدد خاناتها اقل من 1 ولن نرى اعلى من 4 خانات

الان سننفذ الامر فعلا لانشاء هذه القائمة في ملف كما هو موضح:

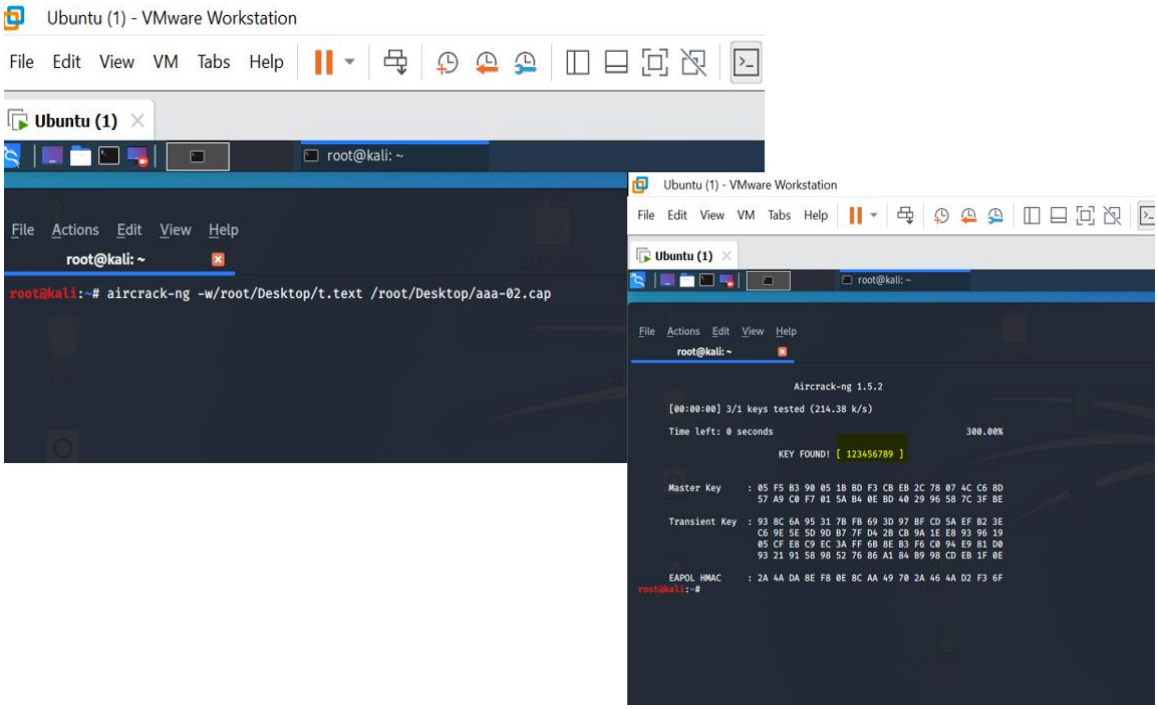




- الان افتح الملف واكتب كلمة المرور الخاص بالاكسس بوينت التي تملكها فيه (كلمة المرور الحقيقية لشبكتك ال wifi)اي قم باضافته في اي مكان في هذا الملف مثلا اخر صف واحفظه:



- اخيرا سنكسر كلمة المرور من خلال الامر المبين في الصورة ادناه حيث انه جرب كلمة مرور في القائمة وقارنها مع ما هو موجود في ملف التقاط الحزم السابق aaa ليكتشف ان كلمة المرور هي النتيجة الظاهرة في الصورة ايضا:



نـهايـة الدليل العمـلـي