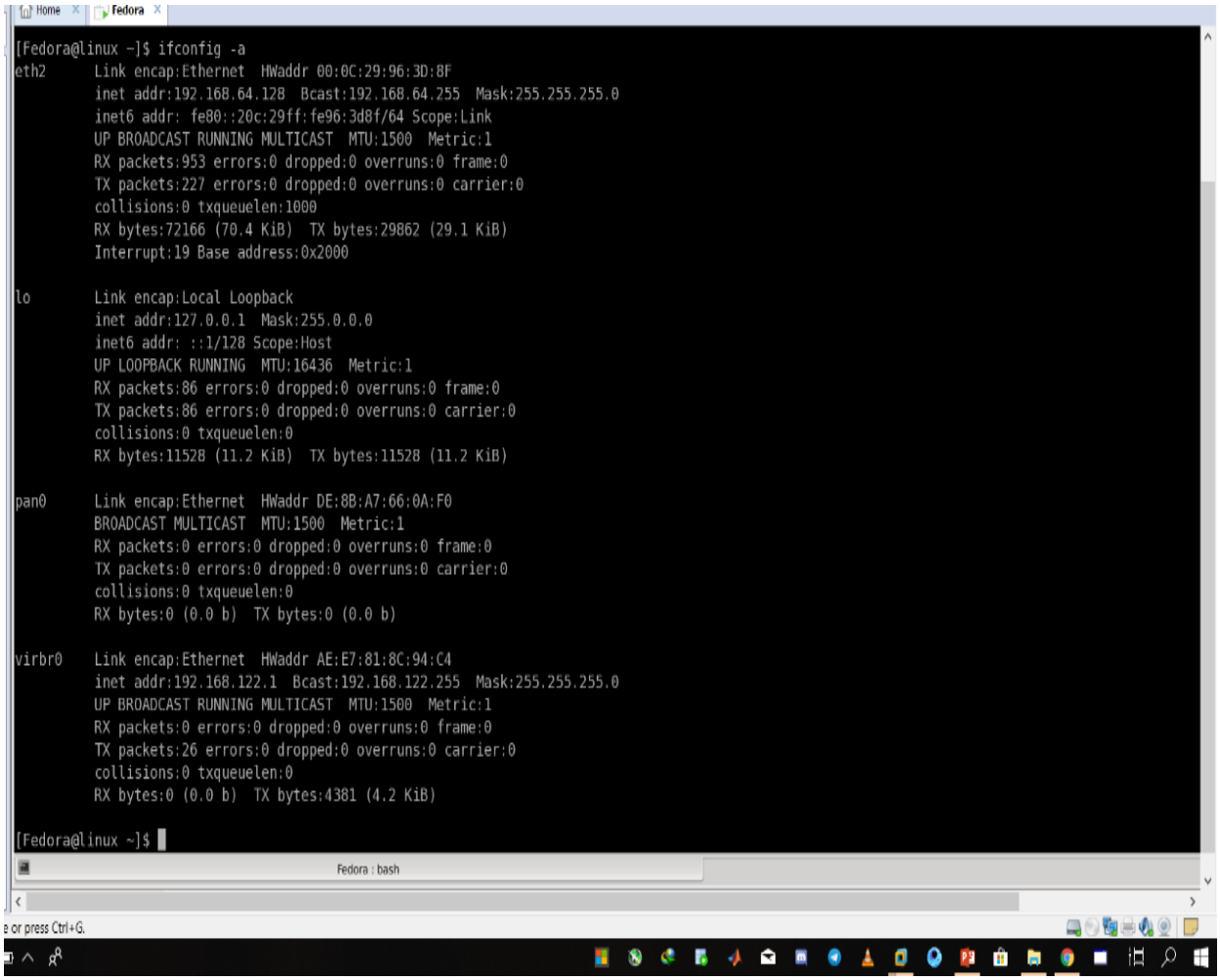
ifconfig

يستخدم من اجل تعيين ip address لأحد المنافذ الخاصة بالشبكة او من اجل استعراض معلومات عن المنافذ الموجودة في الشبكة والتحكم بها.

Ifconfig دون اي بارامتر تعرض لنا المنافذ النشطة فقط

ولعرض جميع المنافذ النشطة والغير نشطة نكتب الأمر : **Ifconfig –a**



لعرض معلومات منفذ معين نكتب:

Ifconfig اسم المنفذ

لإيقاف تفعيل منفذ معين نكتب:

Ifconfig اسم المنفذ down

لتفعيل منفذ معين نكتب:

Ifconfig اسم المنفذ up

اذا اردنا تغيير عنوان ال **ip address** و ال **mask** و ال **Bcast** الخاص بمنفذ ما نكتب :

Ifconfig اسم المنفذ العناوين الجديدة

مثال : تغيير عنوان المنفذ eth2

```
[root@linux Fedora]# ifconfig eth2 10.0.0.1 netmask 255.0.0.0 broadcast 10.255.255.255
[root@linux Fedora]# ifconfig eth2
eth2      Link encap:Ethernet  HWaddr 00:0C:29:42:E4:5A
          inet addr:10.0.0.1  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::20c:29ff:fe42:e45a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:88 errors:0 dropped:0 overruns:0 frame:0
          TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11375 (11.1 KiB)  TX bytes:11843 (11.5 KiB)
          Interrupt:19 Base address:0x2000
```

ما هو الأمر ping وكيف يعمل ؟

هو أمر يقوم بفحص الاتصال مع أجهزة الشبكة او أي موقع على الإنترنت .

يعمل أمر ping على فحص إمكانية الوصول إلى عنوان IP ، مضيف أو خادم انطلاقا من شبكتك.

يكثُر استخدام الأمر للتدقيق في أخطاء الشبكة وتحديد مشاكلها.

المعطى الضروري الوحيد لأمر ping هو اسم المضيف أو عنوان IP المراد فحصُه.

example.com اسم المضيف **ping example.com**

أو من خلال ال IP له **ping 93.184.216.34**

مخرجات الأمر:

PING example.com (93.184.216.34) 56(84) bytes of data.

64 bytes from example.com (93.184.216.34): icmp_seq=1 ttl=42 time=116 ms

64 bytes from example.com (93.184.216.34): icmp_seq=2 ttl=42 time=154 ms

64 bytes from example.com (93.184.216.34): icmp_seq=3 ttl=42 time=163 ms

64 bytes from example.com (93.184.216.34): icmp_seq=4 ttl=42 time=1028 ms

64 bytes from example.com (93.184.216.34): icmp_seq=5 ttl=42 time=768 ms

64 bytes from example.com (93.184.216.34): icmp_seq=6 ttl=42 time=128 ms

لتوقيف تنفيذ الأمر بالضغط على الزرين CTRL و C وإلا فإن الأمر سيستمر في إرسال الحزم.

يظهر ملخّص بالإحصاءات بعد توقف الأمر:

^X^C

--- example.com ping statistics ---

24 packets transmitted, 23 received, 4% packet loss, time 23041ms

rtt min/avg/max/mdev = 114.323/307.465/1057.499/296.627 ms, pipe 2

يتضمن الملخص :

عدد الحزم المُرسَلة Transmitted

عدد الحزم المستلمة Received

نسبة فقدان الحزم Packet loss

الحد الأدنى للمدة الزمنية لوصول الإجابة .min

متوسط وصول الإجابة .avg

الحد الأقصى للمدة الزمنية لوصول الإجابة .max

عدد مرات تنفيذ الأمر

السلوك المبدئي لأمر ping إن استخدم بدون خيارات هو الاستمرار في إرسال الحزم إلى أن يتدخل أحد لإيقافه، إلا أنه توجد طريقة لتحديد عدد مرات إرسال الحزم.

استخدم الخيار c- متبوعا بعدد على النحو التالي:

ping -c 5 example.com

الخرج :

PING example.com (93.184.216.34) 56(84) bytes of data.

64 bytes from example.com (93.184.216.34): icmp_seq=1 ttl=43 time=129 ms

64 bytes from example.com (93.184.216.34): icmp_seq=2 ttl=43 time=127 ms

64 bytes from example.com (93.184.216.34): icmp_seq=3 ttl=43 time=126 ms

64 bytes from example.com (93.184.216.34): icmp_seq=4 ttl=43 time=125 ms

64 bytes from example.com (93.184.216.34): icmp_seq=5 ttl=43 time=284 ms

--- example.com ping statistics ---

5 packets transmitted, 5 received, % packet loss, time 9011ms

rtt min/avg/max/mdev = 125.003/149.335/284.433/47.508 ms

تعديل حجم حزمة البيانات :

يُرسِل أمر ping مبدئيا حزمة بحجم ٦٤ بايت على لينكس، و٣٢ بايت على ويندوز. إن أردت تغيير الحجم المبدئي للحزمة على لينكس فيمكنك ذلك باستخدام الخيار : s-

ping -s 100 -c 4 example.com

الخرج:

PING example.com (93.184.216.34) 100(128) bytes of data.

108 bytes from example.com (93.184.216.34): icmp_seq=2 ttl=51 time=1113 ms

108 bytes from example.com (93.184.216.34): icmp_seq=3 ttl=51 time=253 ms

108 bytes from example.com (93.184.216.34): icmp_seq=4 ttl=51 time=263 ms

--- example.com ping statistics ---

4 packets transmitted, 3received, 16% packet loss, time 4999ms

rtt min/avg/max/mdev = 253.093/590.201/1113.044/408.995 ms, pipe 2

زيادة المدة الزمنية أو تقليصها:

ينتظر أمر ping مبدئيا ثانية واحدة قبل إرسال الحزمة الموالية إلى الوجهة. يمكِّن استخدام الخيار i- من زيادة هذا المجال أو تقليصه.

ping -i 3 example.com

يمكننا بنفس الطريقة التسريع من إرسال الحزم بدل انتظار ثانية في كل مرة:

ping -i 0.2 example.com

عرض إحصاءات ping فقط :

يمكن باستخدام الخيار q- الإبقاء على إحصاءات الأمر فقط دون إظهار معلومات الحزم:

ping -c 5 -q example.com

PING example.com (93.184.216.34) 56(84) bytes of data.

--- example.com ping statistics ---

5 packets transmitted, 4 received, 20% packet loss, time 6221ms

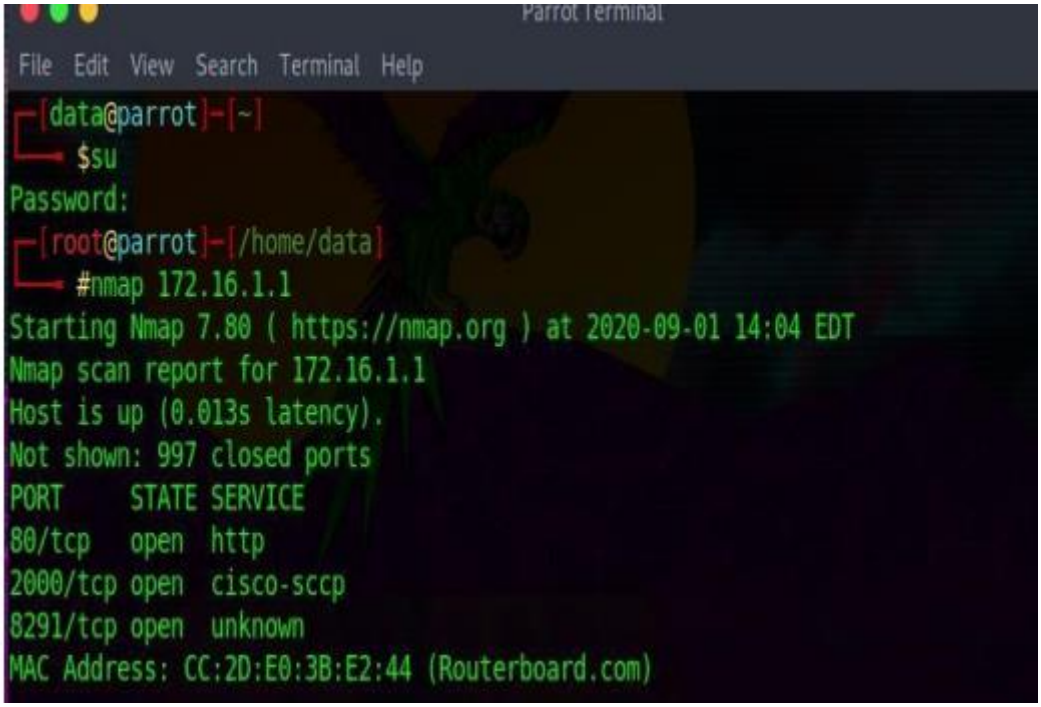
rtt min/avg/max/mdev = 259.175/723.504/1219.311/460.540 ms, pipe 2

يظهر التقرير فقط في مخرجات الأمر أعلاه.

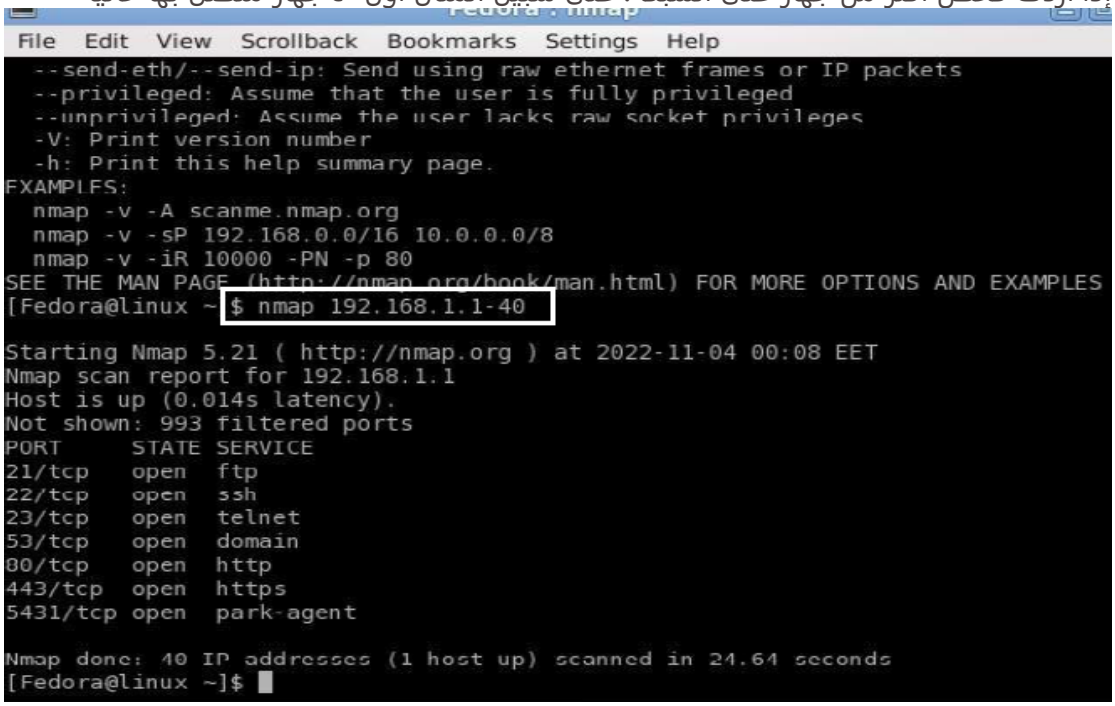
NMAP

(Nmap)، اختصار لـ (Network Mapper) هي أداة مجانية ومفتوحة المصدر تُستخدم لفحص الثغرات الأمنية ومسح المنافذ ورسم خرائط الشبكة.

إذا كنت تريد فقط فحص شبكتك المحلية ومعرفة عدد الأجهزة المتصلة بشبكة Wifi الخاصة بك ، فيمكنك استخدام هذا الأمر. سيعطيك هذا الأمر قائمة بجميع الأجهزة في الشبكة بالإضافة إلى جميع المنافذ المفتوحة لتلك الأجهزة$ nmap 172.16.1.1 .



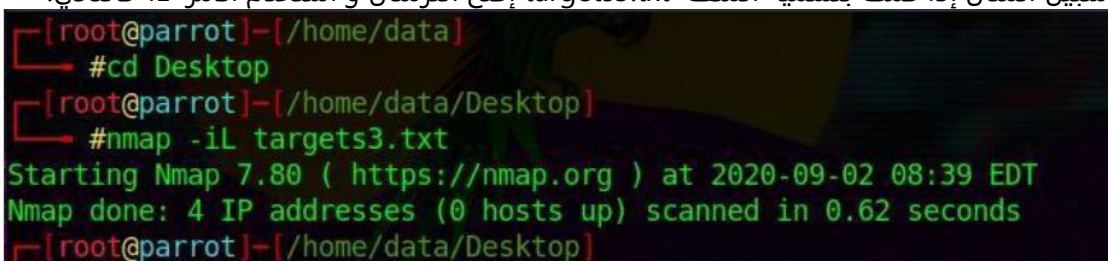
إذا أردت فحص أكثر من جهاز على الشبكة، على سبيل المثال أول ٤٠ جهاز متصل بها حالياً



إذا أردت فحص كامل الشبكة استخدم رمز النجمة * الذي يعني الكل All كالتالي.

nmap 192.168.1.1*

اذا أردت فحص آيبيات محددة، ننشئ ملف txt على سطح المكتب و نكتب فيه الآيبيات ، على سبيل المثال إذا قمت بتسمية الملف targets3.txt إفتح الترمنال و استخدم الأمر iL- كالتالي.



لعمل فحص قوي يسمى فحص عدواني، نستخدم الرمز A- كالتالي مع الإشارة إلى أنه يتطلب وقت أكثر في لإتمام المهمة لأنه يفحص كل شي.

nmap -A 192.168.1.1

لمعرفه نظام تشغيل رواتر او سيرفر موقع معين نستخدم الأمر O- كالتالي.

nmap -O 192.168.1.1

لعمل فحص سريع (ضعيف) يعطي بعض المعلومات فقط و هذه اكثر طريقة مستخدمه

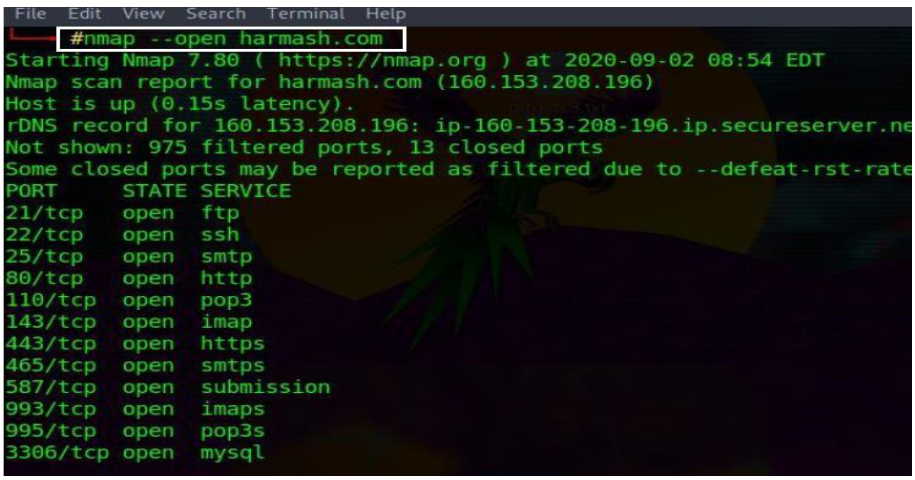
لمعرفه بعض المعلومات السطحية عن الهدف نستخدم الأمر sV- كالتالي.

nmap -sV 192.168.1.1

لفحص بورتات محددة مثلاً البورتات 80و 139و 443 نستخدم p-

nmap -p 80,139,443 192.168.1.1

لعرض البورتات المفتوحة نستخدم الأمر open--



NETSTAT

netstat : هو عبارة عن أمر يستخدم من أجل إظهار معلومات تفصيلية عن الشبكة وعن كيفية اتصال الحاسب مع الأجهزة والشبكات الاخرى.

من المعلومات التي يعرضها الامر:

- عرض اتصالات الشبكة.
- عرض جداول التوجيه.
- عرض تفاصيل كروت الشبكة.

❑ **طريقة التثبيت:**

 # yum install net-tools **من أجل (Fedora)**

 # apt install net-tools **من أجل (Debian)**

يتم تثبيت netstat فقط في حال كانت توزيعه لينكس غير مثبت عليها Netstat.

وسائط netstat:

-i, --interfaces: يستخدم لعرض كافة كروت الشبكة.

-n, --numeric: تعرض عنوان IP بدلا من hostname.

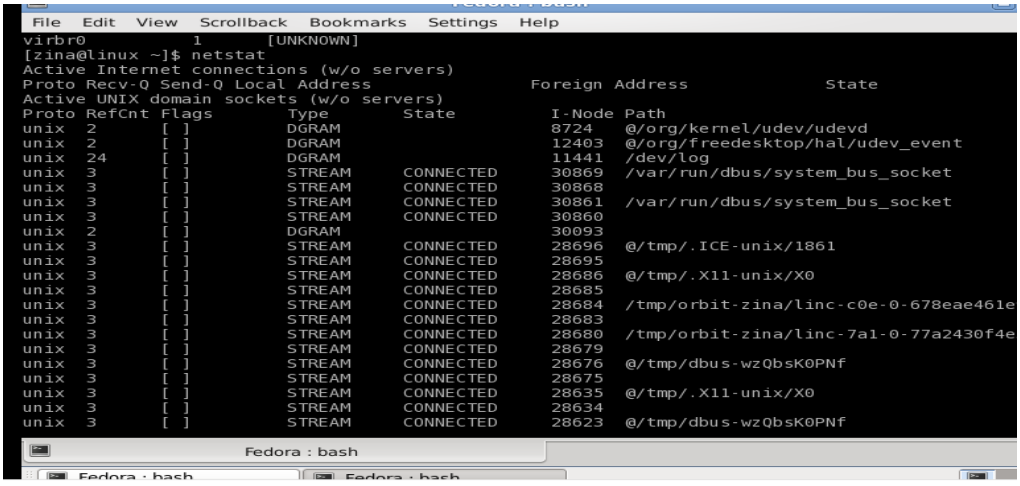
-a, --all: تعرض كل الاتصالات الحالية من مختلف البروتوكولات.

-t, --tcp: تستخدم لعرض اتصالات TCP.

-u, --udp: تستخدم لعرض اتصالات UDP.

-p, --program: يستخدم لعرض (process identifier) PID واسم البرنامج الذي قام بتأسيس الاتصال.

- عند تنفيذ الامر netstat من دون أي وسائط يعرض قائمة من المقابس المفتوحة.



- من أجل عرض كل الاتصالات الحالية من مختلف البرتوكولات الموجودة نستخدم الوسيط «–a».

```
[root@linux Fedora]# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 192.168.122.1:domain        *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 linux.fedora:ipp            *:*                         LISTEN
tcp        0      0 *:36888                     *:*                         LISTEN
tcp        0      0 linux.fedora:smtp           *:*                         LISTEN
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 localhost:ipp               *:*                         LISTEN
tcp        0      0 *:38683                     *:*                         LISTEN
udp        0      0 *:42602                     *:*
udp        0      0 *:sunrpc                    *:*
udp        0      0 *:ipp                       *:*
```

- من أجل عرض كل الاتصالات الحالية من البرتوكول TCP نستخدم الوسيط t-
- **ملاحظة:** يمكن دمج عدة وسائط مثل a– و t– يصبحوا على الشكل التالي at-

```
[root@linux Fedora]# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 192.168.122.1:domain        *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 linux.fedora:ipp            *:*                         LISTEN
tcp        0      0 *:36888                     *:*                         LISTEN
tcp        0      0 linux.fedora:smtp           *:*                         LISTEN
tcp        0      0 *:sunrpc                    *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 localhost:ipp               *:*                         LISTEN
tcp        0      0 *:38683                     *:*                         LISTEN
[root@linux Fedora]#
```

- من أجل عرض كل الاتصالات الحالية من البرتوكول UDP نستخدم الوسيط u-

```
[root@linux Fedora]# netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
udp        0      0 *:42602                     *:*
udp        0      0 *:sunrpc                    *:*
udp        0      0 *:ipp                       *:*
udp        0      0 *:mdns                      *:*
udp        0      0 *:netconfsoapbeep           *:*
udp        0      0 *:895                       *:*
udp        0      0 192.168.122.1:domain        *:*
udp        0      0 *:53823                     *:*
udp        0      0 *:bootps                    *:*
udp        0      0 *:bootpc                    *:*
udp        0      0 *:sunrpc                    *:*
udp        0      0 *:43250                     *:*
udp        0      0 *:netconfsoapbeep           *:*
```

Nslookup

تعليمة تعمل كعمل dns نحصل على اسم الجهاز أو اسم موقع من ip

Nslookup google.com

ipcalc

هناك طريقة تستخدم في العنونة اسمها prefix

192.168.1.0 /24

يكافئ الشبكة التالية

Network 192.168.1.0 mask 255.255.255.0

يستخدم الأمر ipcalc لاستنتاج ال subnet mask و ال Broadcast

مثال نستخدم الأمر ipcalc لحساب الPrefix

ipcalc –p 192.168.1.0 255.255.255.0

وتكون النتيجة هي 24

مثال معاكس استنتاج القناع وعنوان البث وعنوان الشبكة

ipcalc –m –n –b 192.168.1.0/16

وتكون النتيجة

NETMASK=255.255.0.0 BROADCAST=192.168.255.255

NETWORK=192.168.0.0