

dnsmasq: Servizos DNS + DHCP

ESCENARIO

Máquinas virtuais:

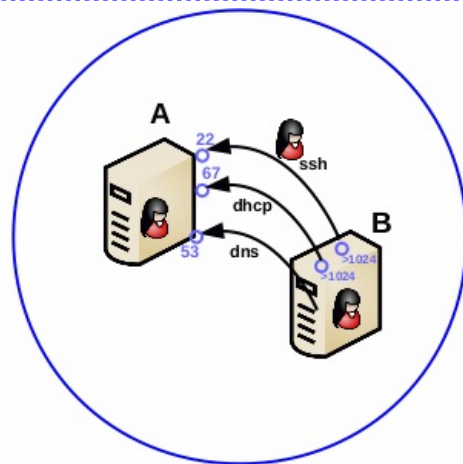
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
Rede: 192.168.120.0

Máquina virtual A:

Rede Interna e NAT
Servidor SSH: openssh-server
Servidor DNS+DHCP: dnsmasq
ISO: Kali Live amd64
IP/MS: 192.168.120.100/24
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

Máquina virtual B:

Rede Interna
Cliente SSH: openssh-client (ssh)
Cliente DHCP: dhclient
ISO: Kali Live amd64
IP/MS: 192.168.120.101/24



NOTAS:

- **dnsmasq** integra un sinxelo servidor DNS e servidor DHCP/TFTP fáciles de implementar. Paquete dnsmasq (# apt update && apt -y install dnsmasq)
- Ficheiros de configuración dnsmasq:
 - Servidor DNS: **/etc/hosts**
 - Servidor DHCP: **/etc/dnsmasq.conf**
- Ficheiro de configuración **/etc/resolv.conf**: Arquivo onde se configuran os servidores DNS que solucionan as peticións de nomes directa ou inversa.
- Cliente DHCP: Comando **dhclient**. Paquete isc-dhcp-client (# apt update && apt -y install isc-dhcp-client).
- Clientes DNS:
 - Comandos **nslookup** e **dig**. Paquete bind9-dnsutils (#apt update && apt -y install bind9-dnsutils)
 - Comando **host**. Paquete bind9-host (#apt update && apt -y install bind9-host)
- Cliente SSH: Comando ssh. Paquete openssh-client (# apt update && apt -y install openssh-client).
- Servidor SSH: Paquete openssh-server (# apt update && apt -y install openssh-server).

Máquina virtual A: Kali amd64

1. Na contorna gráfica abrir un terminal e executar:

```
kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
```

```
kali@kali:~$ passwd kali #Cambiar o contrasinal do usuario kali. Por como contrasinal abc123. (Olo que o contrasinal ten un caracter punto final).
```

2. Cambiar hostname da máquina virtual A. Por kaliA como hostname:

```
kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
```

```
root@kali:~# echo 'kaliA' > /etc/hostname #Indicar ao sistema o valor do hostname.
```

```
root@kali:~# echo 'kernel.hostname=kaliA' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
```

```
root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
```

```
root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
```

```
kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario kali.
```

3. Configurar a rede:

Na contorna gráfica abrir un terminal e executar:

```
kali@kaliA:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
```

```
kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
```

```
root@kaliA:~# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflito con este demo.
```

```
root@kaliA:~# /etc/init.d/network-manager stop #Parar o demo network-manager(xestor de rede) para poder configurar de forma manual a configuración de rede e non ter conflito con este xestor.
```

```
root@kaliA:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo) e interna(eth0).
```

```
root@kaliA:~# ip addr add 192.168.120.100/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.100 e máscara de subrede: 255.255.255.0.
```

```
root@kaliA:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo) e interna(eth0).
```

```
root@kaliA:~# ping -c4 192.168.120.100 #Comprobar mediante o comando ping a conectividade coa interface de rede local eth0
```

4. Comprobar estado do Servidor SSH:

```
root@kaliA:~# /etc/init.d/ssh status #Comprobar o estado do servidor SSH, por defecto non está arrancado.
```

```
root@kaliA:~# nc -vz localhost 22 #Mediante o comando nc(netcat) comprobar se o porto 22 do servidor ssh está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.
```

```
root@kaliA:~# nc -vz 192.168.120.100 22 #Mediante o comando nc(netcat) comprobar se o porto 22 do servidor ssh está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.
```

```
root@kaliA:~# netstat -natp | grep 22 #Mediante o comando netstat comprobar que o porto 22 do servidor SSH está en estado escoita(listen), esperando conexións. A opción -n permite non resolver nomes amosando así soamente as IPs e o comando ser máis rápido na execución. A opción -a equivale á opción all o que permite amosar todos os sockets (conectores) á escoita no servidor. A opción -t equivale a tcp o que permite buscar soamente información sobre o protocolo TCP. A opción -p equivale a program e amosa o PID e nome do programa ao cal pertence o socket.
```

```
root@kaliA:~# ss -natp | grep 22 #Mediante o comando ss comprobar que o porto 22 do servidor SSH está en estado escoita(listen), esperando conexións. A opción -n permite non resolver nomes amosando así soamente as IPs e o comando ser máis rápido na execución. A opción -a equivale á opción all o que permite amosar todos os sockets (conectores) á escoita no servidor. A opción -t equivale a tcp o que permite buscar soamente información sobre o protocolo TCP. A opción -p equivale a program e amosa o PID e nome do programa ao cal pertence o socket.
```

```
root@kaliA:~# /etc/init.d/ssh start #Arrancar o servidor SSH.
```

```
root@kaliA:~# /etc/init.d/ssh status #Comprobar o estado do servidor SSH, agora debe estar arrancado.
```

```
root@kaliA:~# find /etc/rc* -name "*ssh*" #Busca polas links runlevels nos cartafoles /etc/rc*
```

```
root@kaliA:~# systemctl enable ssh #Permite que o servizo ssh sexa iniciado no arranque xerando os links nos runlevels (/etc/rcX.d)
```

```
root@kaliA:~# find /etc/rc* -name "*ssh*" #Busca polas links runlevels nos cartafoles /etc/rc*
```

root@kaliA:~# systemctl is-enabled ssh.service #Amosa se o servizo ssh está enabled ou disabled

root@kaliA:~# nc -vz 192.168.120.100 22 #Mediante o comando nc(netcat) comprobar se o porto 22 do servidor ssh está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.

root@kaliA:~# ssh -v kali@localhost #Comprobar se o servidor SSH está activo e podemos conectarnos a el dende localhost co usuario kali e o seu contrasinal. Se é a primeira vez que nos conectamos o servidor avísanos se estamos de acordo coa autenticación. Respostamos yes e pulsamos Enter. A opción -v (modo verbose) aporta información máis detallada da conexión.

kali@kaliA:~\$ exit #Saír da consola remota ssh a que acabamos de acceder, para voltar á consola local de **root**.

root@kaliA:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de **kali**.

kali@kaliA:~\$

Máquina virtual B: Kali amd64

5. Configuración da rede. Na contorna gráfica abrir un terminal e executar:

```
kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
```

```
kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
```

```
root@kali:~# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflito con este demo.
```

```
root@kali:~# /etc/init.d/network-manager stop #Parar o demo network-manager(xestor de rede) para poder configurar de forma manual a configuración de rede e non ter conflito con este xestor.
```

```
root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina B as tarxetas de redes: loopback(lo) e interna(eth0).
```

```
root@kali:~# ip addr add 192.168.120.101/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.101 e máscara de subrede: 255.255.255.0.
```

```
root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina B as tarxetas de redes: loopback(lo) e interna(eth0).
```

```
root@kali:~# ping -c4 192.168.120.101 #Comprobar mediante o comando ping a conectividade coa interface de rede local eth0
```

```
root@kali:~# ping -c4 192.168.120.100 #Comprobar mediante o comando ping a conectividade coa interface de rede da máquina virtual A
```

```
root@kali:~# echo '192.168.120.100 kaliA' >> /etc/hosts #Engadir no ficheiro /etc/hosts, é dicir, na táboa estática de búsqueda para nomes de host (DNS) o nome kaliA, para que atenda á IP 192.168.120.100
```

```
root@kali:~# ping -c4 kaliA #Comprobar mediante o comando ping a conectividade coa interface de rede da máquina virtual A
```

6. Cambiar hostname da máquina virtual B. Por kaliB como hostname:

```
root@kali:~# echo 'kaliB' > /etc/hostname #Indicar ao sistema o valor do hostname.
```

```
root@kali:~# echo 'kernel.hostname=kaliB' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
```

```
root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
```

```
root@kali:~# exit #Sair da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
```

```
kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario kali.
```

7. ^{SSH} **B → A** Acceder mediante SSH dende a máquina virtual B á máquina virtual A. Dende agora executaremos sempre os comandos dende a máquina virtual B, a través da consola SSH:

Na contorna gráfica abrir un terminal e executar:

```
kali@kaliB:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
```

```
kali@kaliB:~$ nc -vz 192.168.120.100 22 #Mediante o comando nc(netcat) comprobar que o porto 22 do servidor SSH está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.
```

```
kali@kaliB:~$ nc -vz kaliA 22 #Mediante o comando nc(netcat) comprobar que o porto 22 do servidor SSH está en estado escoita(listen), esperando conexións. A opción -v corresponde á opción verbose, o que permite amosar información máis detallada na saída do comando. A opción -z permite devolver PROMPT do sistema e de igual xeito facer o escaneo ao/s porto/s solicitados. O número 22 é o porto TCP a escanear.
```

```
kali@kaliB:~$ ssh -v kali@192.168.120.100 #Comprobar se o servidor SSH está activo e podemos conectarnos a el. Agora accedemos como o usuario kali a través da conexión cifrada SSH.
```

```
kali@kaliA:~$
```

8. Instalar dnsmasq (DNS + DHCP):

```
kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co
comando sudo (/etc/sudoers, visudo)
root@kaliA:~# apt update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list,
/etc/apt/sources.list.d/)
root@kaliA:~# apt search dnsmasq #Buscar calquera paquete que coincida co patrón de búsqueda
dnsmasq
root@kaliA:~# apt -y install dnsmasq #Instalar o paquete dnsmasq. Co parámetro -y automaticamente
asumimos yes a calquera pregunta que ocorra na instalación do paquete.
```

9. Habilitar servizo dnsmasq(DNS + DHCP):

```
root@kaliA:~# /etc/init.d/dnsmasq status #Comprobar o estado do servidor dnsmasq
root@kaliA:~# /etc/init.d/dnsmasq start #Arrancar o servidor dnsmasq.
root@kaliA:~# /etc/init.d/dnsmasq status #Comprobar o estado do servidor dnsmasq
```

10. dnsmasq como servidor DNS

a. /etc/resolv.conf e /etc/hosts:

Para que dnsmasq poida realizar a resolución directa ou inversa de hostnames/IPs simplemente temos que engadir/modificar entradas no ficheiro /etc/hosts e indicarlle ao arquivo /etc/resolv.conf cal é o noso servidor DNS a empregar.

/etc/resolv.conf: Arquivo onde se configuran os servidores DNS. Exemplo contido tipo:

```
domain example.local #Dominio a engadir na procura de hostnames. Se o host a buscar é pepito,
é a procura falla, intentariase de novo esta como pepito.example.local

search example.local #Lista de dominios a engadir na procura de hostnames.

nameserver 8.8.8.8 #Servidor DNS primario para resolución de nomes.

nameserver 8.8.4.4 #Agrega servidor DNS secundario para resolución de nomes.
```

domain e search son excluintes, a última directiva que apareza no ficheiro prevalece.

```
root@kaliA:~# echo -e 'nameserver 127.0.0.1\nnameserver 192.168.120.100' >
/etc/resolv.conf #Agrega servidor DNS para resolución de nomes.
root@kaliA:~# echo '192.168.120.100 kaliA.ies.local kaliA.ies.com
kaliA.example.local kaliA.example.gl' >> /etc/hosts #Engadir no ficheiro /etc/hosts, é dicir, na
táboa estática de búsqueda para nomes de host (DNS) varios nomes DNS que apuntan á IP 192.168.120.100
root@kaliA:~# echo '192.168.120.101 kaliB.ies.local kaliB.ies.com
kaliB.example.local kaliB.example.gl' >> /etc/hosts #Engadir no ficheiro /etc/hosts, é dicir, na
táboa estática de búsqueda para nomes de host (DNS) varios nomes DNS que apuntan á IP 192.168.120.101
```

b. Comprobación resolución DNS: DNS en /etc/hosts

Á hora de saber se tes conectividade con algunha máquina na internet, ou en rede local, adóitase utilizar o comando ping, o cal indica segundo a súa resposta se posúes conectividade coa máquina en cuestión. O comando ping pódolo utilizar para consultar direccións IP ou nomes de dominios. Por tanto o comando ping debe ser capaz de consultar información sobre o sistema de nomes de dominio; é un resolutor, un programa cliente capaz de consultar información sobre o sistema de nome de dominios. Normalmente, un resolutor traballa discretamente en segundo plano e os usuarios non coñecen a súa presenza, é dicir, que toda consulta dun cliente DNS ao seu servidor adoita realizala o programa que invocamos (ping, ftp, telnet, mail, navegador web, etc.). Por exemplo, se solicitas unha conexión ftp a ftp.rediris.es, a aplicación ftp que empregues chama a un programa resolutor local que busca a dirección IP dese computador 130.206.13.2 sen que teñas conciencia diso, isto é, para ti o proceso é transparente. Ademais deste traballo en segundo plano, o usuario pode conectarse directamente ao programa resolutor enviando consultas e resolvendo respostas. Comandos resolutor típicos en sistemas operativos GNU/Linux son: nslookup, host e dig.

```
root@kaliA:~# ping -c4 kaliA.ies.local #Comprobar mediante o localando ping a conectividade co
host kaliA.ies.local que apunta á interface de rede da máquina virtual A
root@kaliA:~# ping -c4 kaliA.ies.com #Comprobar mediante o comando ping a conectividade co
host kaliA.ies.com que apunta á interface de rede da máquina virtual A
```

```

root@kaliA:~# ping -c4 kaliA.example.local #Comprobar mediante o comando ping a
conectividade co host kaliA.example.local que apunta á interface de rede da máquina virtual A
root@kaliA:~# nslookup kaliA.example.gl #Resolución directa: Consultar a dirección IP do host
kaliA.example.gl
root@kaliA:~# host kaliA.ies.com #Comando equivalente ao anterior
root@kaliA:~# dig kaliA.ies.com #Comando equivalente ao anterior
root@kaliA:~# nslookup 192.168.120.100 #Resolución inversa: Consultar o nome do host que
posúe a dirección IP 192.168.120.100
root@kaliA:~# host 192.168.120.100 #Comando equivalente ao anterior
root@kaliA:~# dig -x 192.168.120.100 #Comando equivalente ao anterior

```

Máquina virtual B: Kali amd64

11. Apuntar ao DNS (dnsmasq en kaliA). Modificar `/etc/resolv.conf` e `/etc/hosts`:

a. `/etc/resolv.conf` e `/etc/hosts`:

Para que poidamos empregar dnsmasq como servidor de nomes, e así poida realizar a resolución directa ou inversa de hostnames/IPs, simplemente temos que indicarlle ao arquivo `/etc/resolv.conf` de KaliB cal é o noso servidor DNS a empregar.

```

root@kaliA:~# exit #Saír da consola remota ssh a que acabamos de acceder, para voltar á consola
local de root.
kali@kaliA:~$ exit #Pechar o terminal saíndo da consola local do usuario kali.
kali@kaliB:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos
configurados co comando sudo (/etc/sudoers, visudo)
root@kaliB:~# echo 'nameserver 192.168.120.100' > /etc/resolv.conf #Agregar
servidor DNS para resolución de nomes.

```

b. Comprobación resolución DNS:

```

root@kaliB:~# ping -c4 kaliA #Comprobar mediante o comando ping a conectividade coa interface de
rede da máquina virtual A
root@kaliB:~# ping -c4 kaliA.ies.local #Comprobar mediante o localando ping a conectividade co host
kaliA.ies.local que apunta á interface de rede da máquina virtual A
root@kaliB:~# ping -c4 kaliA.ies.com #Comprobar mediante o comando ping a conectividade co host
kaliA.ies.com que apunta á interface de rede da máquina virtual A
root@kaliB:~# ping -c4 kaliA.example.local #Comprobar mediante o comando ping a conectividade co
host kaliA.example.local que apunta á interface de rede da máquina virtual A
root@kaliB:~# nslookup kaliA.example.gl #Resolución directa: Consultar a dirección IP do host
kaliA.example.gl
root@kaliB:~# host kaliA.ies.com #Comando equivalente ao anterior
root@kaliB:~# dig kaliA.ies.com #Comando equivalente ao anterior
root@kaliB:~# nslookup 192.168.120.100 #Resolución inversa: Consultar o nome do host que posúe a
dirección IP 192.168.120.100
root@kaliB:~# host 192.168.120.100 #Comando equivalente ao anterior
root@kaliB:~# dig -x 192.168.120.100 #Comando equivalente ao anterior

```


Máquina virtual A: Kali amd64

12. dnsmasq como servidor DHCP → /etc/dnsmasq.conf

Por defecto dnsmasq non activa o servidor DHCP. Entón para activalo debemos editar o arquivo de configuración /etc/dnsmasq.conf e configurar un pool de IPs a servir, isto é, configurar os rangos de IPs que queremos conceder para poder distribuír unha IP nunha solicitude dun cliente DHCP.

```
root@kaliA:~# echo 'dhcp-range=192.168.120.50,192.168.120.80,12h' >>
/etc/dnsmasq.conf #Crear rango de IPs a distribuír [50-80]. A concesión durará 12 horas.
root@kaliA:~# /etc/init.d/dnsmasq restart #Reiniciar o servidor dnsmasq.
root@kaliA:~# /etc/init.d/dnsmasq status #Comprobar o estado do servidor dnsmasq
```

Máquina virtual B: Kali amd64

13. dnsmasq como servidor DHCP → Solicitar IP a dnsmasq

```
root@kaliB:~# dhclient -v eth0 #Configuración dinámica de rede da interface eth0 en modo
verbose(detallado).
root@kaliB:~# ip addr show eth0 #Amosara configuración da interface eth0
root@kaliB:~# dhclient -s 192.168.120.100 -v eth0 #Configuración dinámica de rede da interface
eth0 en modo verbose(detallado), procurando a configuración no servidor DHCP 192.168.120.100
root@kaliB:~# ip addr show eth0 #Amosara configuración da interface eth0
```

Ricardo Feijoo Costa



This work is licensed under a **Creative Commons Attribution-ShareAlike 4.0 International License**