GESTIÓ DE XARXES

Lliurament 2

Gestió de Sistemes i Xarxes

URV 2018

Cristòful Daudén Esmel
Aleix Mariné Tena
Josep Marín Llaó

Índex

Lab Servei DNS avançat

Objectiu:

L'objectiu d'aquest laboratori és ampliar el servei DNS per a donar-li un extra de seguretat. Ha de fer un servei Stealth, amb visions diferents per a l'interior i l'exterior i alhora registri els noms assignats pel DHCPd.

Decisions de disseny:

Per major seguretat canviarem les opcions del servidor DNS per a que només serveixi queries recursius des de la intranet dels usuaris i sols es puguin fer transferència de zona des del localhost.
Aprofitarem l'estructura de l'entrega anterior on ja teniem montat el servidor DHCP, el servidor DNS i la VLAN.
A més, enlloc de montar únicament 2 vistes (internal i external), hem decidit montar-ne una tercera per a les màquines de la DMZ, de forma que només puguin accedir als clients de la xarxa interna a través de la VLAN.

Configuració:

Correm el mateix scrip que en la fase anterior amb estructura:

Estructura de l'script

```
function display_help(){
}
function router_config(){
}
function client_config(){
}
function server_config(){
}
while getopts :h option
do
      case "$option" in
      h)
            display_help
            exit 1
      ;;
      *)
            echo "ERROR: Invalid parameters" >&2
            display_help
            exit 1
      ;;
  esac
done
```

```
case "$1" in
      router)
      router_config $*
      exit 0
      ;;
      client)
      client_config $*
      exit 0
      ;;
      server)
      server_config $*
      exit 0
      ;;
      *)
      echo -e "ERROR: machine indication needed:\n\trouter\n\tclient\n\tserver"
      exit 1
esac
```

Configuració router:

En el router executem el següent codi, la part subratllada en groc és la que fa referència a la configuració del DNS.

- Previament, en els fitxers db.externa i externa.db hem de escriure la IP pública actual del servidor.

Primer afegim en els servidors DNS als que consulta el router per resoldre una query a una IP de fora de la xarca en el fitxer /etc/bind/named.conf.options per a que el client i el servidor també puguin resoldre aquestes querys.
Modifiquem el fitxer /etc/bind/named.conf.local on hi ha definida la configuració del nou servidorr DNS amb el model de views.
Copiem els diferents fitxers de zona en el directori /var/cache/bind/.
Afegim la IP 127.0.0.1 en la primera linia del fitxer /etc/resolv.conf per a que el router també resolgui les consultes en el servidor DNS configurat.
Finalment, engeguem el servei.

- També hem de comentar la línea /etc/bind/named.conf.default-zones en el fitxer /etc/bind/named.local

Codi router

```
if [ $# -lt 4 ]
then
      echo "Usem la configuració per defecte"

      #Llistem les interfícies de xarxa
      interfaces=$(ip addres show | egrep -e "^[0-9]" | cut -d ':' -f2 | tr -d '
' | sed '/lo/d')
      i1=$(echo $interfaces | cut -d ' ' -f1)
      i2=$(echo $interfaces | cut -d ' ' -f2)
      i3=$(echo $interfaces | cut -d ' ' -f3)

else
      i1=$2
      i2=$3
      i3=$4
```

```
fi

#revisar la configuració de l'adreça
config="auto lo\niface lo inet loopback
	\n
	\nauto $i1\niface $i1 inet dhcp
	\n
	\nallow-hotplug $i2\niface $i2 inet static\n\taddress
172.17.2.1\n\tnetmask 255.255.255.0\n\tnetwork 172.17.2.0\n\tbroadcast
172.17.2.255
	\n
	\nallow-hotplug $i3\niface $i3 inet static\n\taddress
192.168.8.1\n\tnetmask 255.255.254.0\n\tnetwork 192.168.8.0\n\tbroadcast
192.168.9.255"

cp -p dhcpd.conf /etc/dhcp/dhcpd.conf

sed -i "s/INTERFACES=\".*\"/INTERFACES=\"$i2 $i3\"/g"
"/etc/default/isc-dhcp-server"
#Apaguem les interfícies de xarxa
ifdown $i1 --force
ifdown $i2 --force
ifdown $i3 --force

#S'escriuen els canvis en el fitxer /etc/network/interfaces
echo -e $config > /etc/network/interfaces

#Activem el forwarding
echo 1 >/proc/sys/net/ipv4/ip_forward

echo -e "options{\n\tdirectory \"/var/cache/bind\";\n\tforwarders {" >
/etc/bind/named.conf.options
IFS=$'\n'
for line in $(cat /etc/resolv.conf)
do
	if [ "$(echo $line | egrep -e "[0-9].*")" != "" ]
	then
		echo -e "\t\t$(echo $line | egrep -e "[0-9].*" | cut -d ' ' -f2);"
>> /etc/bind/named.conf.options
	fi
done
echo -e "\t};\n};" >> /etc/bind/named.conf.options

cp named.conf.local /etc/bind/named.conf.local

cp DMZ_2.gsx.db /var/cache/bind/DMZ_2.gsx.db
cp INTRANET.db /var/cache/bind/INTRANET.db
cp db.192.168.9 /var/cache/bind/db.192.168.9
cp db.192.168.8 /var/cache/bind/db.192.168.8
cp db.172 /var/cache/bind/db.172

cp db.externa /var/cache/bind/db.externa
cp externa.db /var/cache/bind/externa.db

cp db.192.168.250 /var/cache/bind/db.192.168.250
cp VLAN.db /var/cache/bind/VLAN.db
```

```
#reiniciem les interficies de xarxa
ifup $i1
ifup $i2
ifup $i3

#obtenim la ip amb conexio a internet del router
addres=$(hostname -I | cut -d ' ' -f1)
echo "Comprovar que la IP esterna és $addres"

#permetem el tràfic cap a l'exterior
iptables -I INPUT -j ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.8.0/23 -j SNAT --to $addres
iptables -t nat -A POSTROUTING -s 172.17.2.0/24 -j SNAT --to $addres

sed -e '1i nameserver 127.0.0.1' /etc/resolv.conf > resolv.conf
cp resolv.conf /etc/resolv.conf
rm resolv.conf

/etc/init.d/bind9 restart
```

El fitxer /etc/bind/named.conf.local on hi ha definides les diferents vistes i zones serà el següent:

```
#Options {
#    directory "/etc/namedb";
#    allow-query-cache { none; };
#    allow-query { any; };
#    recursion no;
#};

view "internal"{
    match-clients { 192.168.8.0/23; localhost; };
    recursion yes;

    zone "interna" {
       type master;
       file "INTRANET.db";
    };

    zone 8.168.192.in-addr.arpa{
       type master;
       file "db.192.168.8";
    };

    zone 9.168.192.in-addr.arpa{
       type master;
       file "db.192.168.9";
    };

    zone "grup2.gsx" {
       type master;
       file "DMZ_2.gsx.db";
    };

    zone 2.17.172.in-addr.arpa {
       type master;
```

```
        file "db.172";
    };

    zone "serveis.interna" {
        type master;
        file "VLAN.db";
    };

    zone 250.168.192.in-addr.arpa{
        type master;
        file "db.192.168.250";
    };

    include "/etc/bind/named.conf.default-zones";
};

view "DMZ"{
    match-clients { 172.17.2.0/24; };
    recursion yes;

    zone "grup2.gsx" {
        type master;
        file "DMZ_2.gsx.db";
    };

    zone 2.17.172.in-addr.arpa {
        type master;
        file "db.172";
    };

    zone "serveis.interna" {
        type master;
        file "VLAN.db";
    };

    zone 250.168.192.in-addr.arpa{
        type master;
        file "db.192.168.250";
    };
};

view "external"{
    match-clients { any; };
    recursion yes;

    zone "grup2.gsx" {
        type master;
        file "externa.db";
    };

    #mirar la ip externa del router
    zone 10.in-addr.arpa {
        type master;
        file "db.externa";
    };
};
```

Els diferents fitxers de zona indicats en el fitxer anterior no s'especifiquen en l'informe, s'adjuntaràn en el comprimit de la pràctica.

Configuració client i servidor:

En el client i servidor no hem d'afegir cap configuració respecte la fase anterior, executare el mateix codi

Codi client (el del servidor només varía amb les IPs)

```
if [ $# -lt 2 ]
then
      echo "Usem la configuració per defecte"

      #Llistem les interfícies de xarxa
      interfaces=$(ip addres show | egrep -e "^[0-9]" | cut -d ':' -f2 | tr -d '
' | sed '/lo/d')
      i1=$(echo $interfaces | cut -d ' ' -f1)
else
      i1=$2
fi

config="auto lo\niface lo inet loopback
      \n
      \nallow-hotplug $i1\niface $i1 inet dhcp"

ifdown $i1 --force

#S'escriuen canvis en el fitxer /etc/network/interfaces
echo -e $config > /etc/network/interfaces

#echo -e "domain INTRANET\nsearch INTRANET\nnameserver 192.168.8.1" >
/etc/resolv.conf

#S'afegeixen les rutes que calguin
echo "up ip route add 172.17.2.0/24 via 192.168.8.1 dev $i1" >>
/etc/network/interfaces
echo "up ip route add default via 192.168.8.1" >> /etc/network/interfaces

ifup $i1
}
```

Possibles errors:

A l'hora de provar els scripts de configuració hem detectat els següents errors:

- No d'inicia correctament el servei isc-dhcp-server:
  - eliminar el fitxer /var/run/dhcp.pid
  - matar els processos dhcp
  - especificar les interfícies a les que donem servei en el /etc/default/dhcp.conf
  - sudo /etc/init.d/isc-dhcp-server stop
  - sudo /etc/init.d/isc-dhcp-server stop
- Si no pots fer ping a google en client i servidor:
  - comprovar en les iptables que la traducció en el SNAT sigui correcta.

- Si el servei bind9 dona error:
    - resvisar si és corecta la IP pública del router en el fitxers de zona de db.externa i externa.db
    - comentar la línea indicada anteriorment en el fitxer /etc/bind/named.conf

Joc de Proves

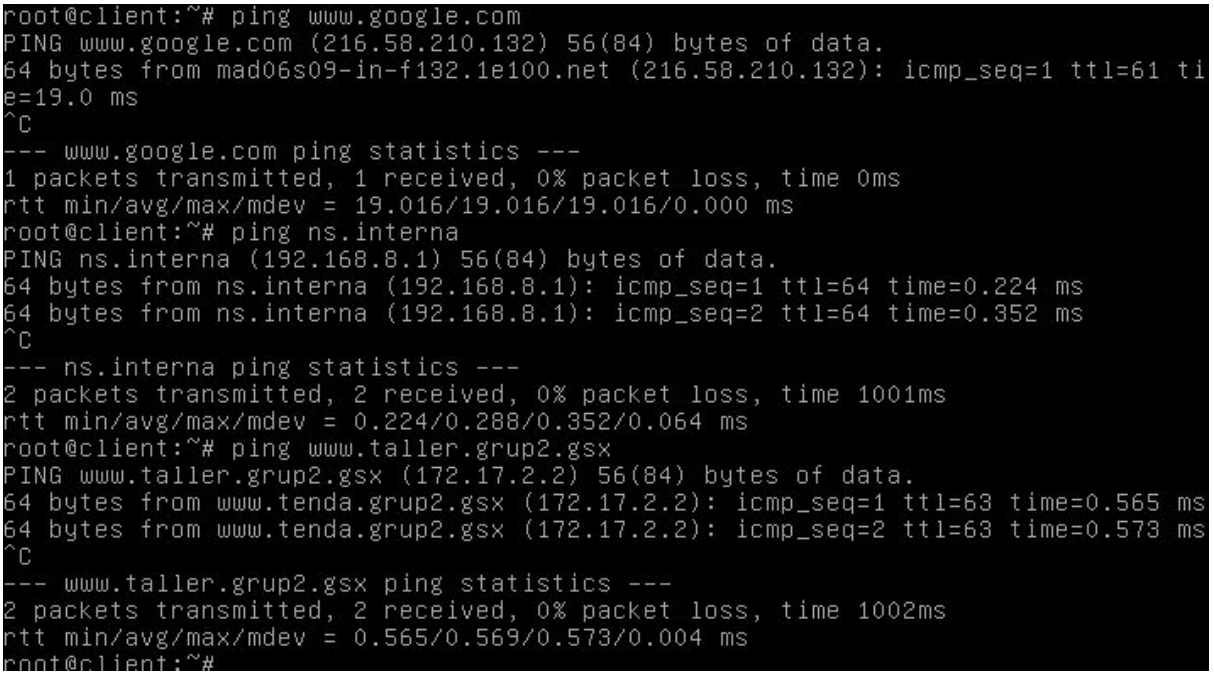
Primer hem comprovat que la traducció de noms cap a client i servidor sigui correcta en el router mitjançant l'eina dig.
Com és pot observar fa correctament les traduccions dels noms de domini pc1.interna i www.taller.grup2.gsx:

```
root@casa:/home/milax/GSX_Labs/Prac2Xarxes# dig pc1.interna

; <<>> DiG 9.9.5-9+deb8u15-Debian <<>> pc1.interna
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10183
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;pc1.interna.                   IN      A

;; ANSWER SECTION:
pc1.interna.            604800  IN      A       192.168.8.2

;; AUTHORITY SECTION:
interna.                604800  IN      NS      ns.interna.

;; ADDITIONAL SECTION:
ns.interna.             604800  IN      A       192.168.8.1

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu May 24 20:36:56 CEST 2018
;; MSG SIZE  rcvd: 89
```

```
root@casa:/home/milax/GSX_Labs/Prac2Xarxes# dig www.taller.grup2.gsx

; <<>> DiG 9.9.5-9+deb8u15-Debian <<>> www.taller.grup2.gsx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11771
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.taller.grup2.gsx.          IN      A

;; ANSWER SECTION:
www.taller.grup2.gsx.   604800  IN      A       172.17.2.2

;; AUTHORITY SECTION:
grup2.gsx.              604800  IN      NS      ns.grup2.gsx.

;; ADDITIONAL SECTION:
ns.grup2.gsx.           604800  IN      A       172.17.2.1

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu May 24 20:37:47 CEST 2018
;; MSG SIZE  rcvd: 98
```

Després des del servidor hem comprovat que el router en doni el servei DNS realitzant pings als noms de dominis de les màquines router i client. Alhora, també hem comprovat que en el router estigui el SNAT ben configurat fent ping a www.google.com. Hem realitzat el mateix procés des de la màquina client.

```
root@server:~# ping www.google.es
PING www.google.es (216.58.211.35) 56(84) bytes of data.
64 bytes from mad08s05-in-f3.1e100.net (216.58.211.35): icmp_seq=1 ttl=61 time=1
6.0 ms
^C
--- www.google.es ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 16.060/16.060/16.060/0.000 ms
root@server:~# ping pc1.interna
PING pc1.interna (192.168.8.2) 56(84) bytes of data.
64 bytes from 192.168.8.2 (192.168.8.2): icmp_seq=1 ttl=63 time=0.464 ms
64 bytes from 192.168.8.2 (192.168.8.2): icmp_seq=2 ttl=63 time=0.558 ms
^C
--- pc1.interna ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.464/0.511/0.558/0.047 ms
root@server:~# ping ns.grup2.gsx
PING ns.grup2.gsx (172.17.2.1) 56(84) bytes of data.
64 bytes from ns.grup2.gsx (172.17.2.1): icmp_seq=1 ttl=64 time=0.252 ms
64 bytes from ns.grup2.gsx (172.17.2.1): icmp_seq=2 ttl=64 time=0.322 ms
^C
--- ns.grup2.gsx ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.252/0.287/0.322/0.035 ms
root@server:~# _
```



Finalment, en el laboratori hem comprovat que des d'una màquina externa a la nostra xarxa, es pugui fer ping al servidor a través del nom de domini www.taller.grup2.gsx. Tot i això, no disposem de cap captura per adjuntar al informe. Si més no, en les següents etapes queda demostrat com hem acoseguit accedir des d'una màquina del laboratori, externa a la xarxa, al servei web apache ofert per la nostra màquina servidor a través del nom de domini esmentat, per lo que queda demostrat que el DNS avançat està ben configurat.

Lab Tallafocs, NAT i servei SSH

Objectiu:

L'objectiu d'aquest laboratori és activar el servei ssh al client, router i servidor de la DMZ, per tal de poder obrir shells remotament i configurar-los. A més, també activarem la SNAT per tal que els ordinadors interns es puguin comunicar amb Internet i la DNAT per a que des de fora es pugui accedir als servidors de la DMZ.
Com a part opcional s'estableixen les regles mínimes de tallafocs al router.

Decisions de disseny:

Aprofitarem l'script del laboratori anterior. La configuració del servei ssh es durà a terme mitjançant l'execució d'un script diferent.

Configuració:

En el script de la fase anterior afegim la configuració de la DNAT en els iptables, s'observa el canvi en el script remarcat en groc (la SNAT no fa falta configurar-la ja que ja ho vam fer el primer dia):

codi client

```
if [ $# -lt 4 ]
then
      echo "Usem la configuració per defecte"

      #Llistem les interfícies de xarxa
      interfaces=$(ip addres show | egrep -e "^[0-9]" | cut -d ':' -f2 | tr -d '
' | sed '/lo/d')
      i1=$(echo $interfaces | cut -d ' ' -f1)
      i2=$(echo $interfaces | cut -d ' ' -f2)
      i3=$(echo $interfaces | cut -d ' ' -f3)

else
      i1=$2
      i2=$3
      i3=$4
fi

#revisar la configuració de l'adreça
config="auto lo\niface lo inet loopback
      \n
      \nauto $i1\niface $i1 inet dhcp
      \n
      \nallow-hotplug $i2\niface $i2 inet static\n\taddress
172.17.2.1\n\tnetmask 255.255.255.0\n\tnetwork 172.17.2.0\n\tbroadcast
172.17.2.255
      \n
```

```
      \nallow-hotplug $i3\niface $i3 inet static\n\taddress
192.168.8.1\n\tnetmask 255.255.254.0\n\tnetwork 192.168.8.0\n\tbroadcast
192.168.9.255"

cp -p dhcpd.conf /etc/dhcp/dhcpd.conf

sed -i "s/INTERFACES=\".*\"/INTERFACES=\"$i2 $i3\"/g"
"/etc/default/isc-dhcp-server"

#Apaguem les interfícies de xarxa
ifdown $i1 --force
ifdown $i2 --force
ifdown $i3 --force

#Escrivim canvis en el fitxer /etc/network/interfaces
echo -e $config > /etc/network/interfaces

#Activem el forwarding
echo 1 >/proc/sys/net/ipv4/ip_forward

echo -e "options{\n\tdirectory \"/var/cache/bind\";\n\tforwarders {" >
/etc/bind/named.conf.options
IFS=$'\n'
for line in $(cat /etc/resolv.conf)
do
      if [ "$(echo $line | egrep -e "[0-9].*")" != "" ]
      then
            echo -e "\t\t$(echo $line | egrep -e "[0-9].*" | cut -d ' ' -f2);"
>> /etc/bind/named.conf.options
      fi
done
echo -e "\t};\n};" >> /etc/bind/named.conf.options

cp named.conf.local /etc/bind/named.conf.local

cp DMZ_2.gsx.db /var/cache/bind/DMZ_2.gsx.db
cp INTRANET.db /var/cache/bind/INTRANET.db
cp db.192.168.9 /var/cache/bind/db.192.168.9
cp db.192.168.8 /var/cache/bind/db.192.168.8
cp db.172 /var/cache/bind/db.172

cp db.externa /var/cache/bind/db.externa
cp externa.db /var/cache/bind/externa.db

cp db.192.168.250 /var/cache/bind/db.192.168.250
cp VLAN.db /var/cache/bind/VLAN.db

#Reiniciem les interficies de xarxa
ifup $i1
ifup $i2
ifup $i3

#Obtenim la ip amb conexio a internet del router
addres=$(hostname -I | cut -d ' ' -f1)
echo "Comprovar que la IP esterna és $addres"
```

```
#Permetem el tràfic cap a l'exterior
iptables -I INPUT -j ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.8.0/23 -j SNAT --to $addres
iptables -t nat -A POSTROUTING -s 172.17.2.0/24 -j SNAT --to $addres
iptables -t nat -A PREROUTING -i $i1 -p tcp --dport 80 -j DNAT --to-destination
172.17.2.2:80
iptables -t nat -A PREROUTING -i $i1 -p tcp --dport 443 -j DNAT --to-destination
172.17.2.2:443
iptables -t nat -A PREROUTING -i $i1 -p tcp --dport 23 -j DNAT --to-destination
172.17.2.2:22

sed -e '1i nameserver 127.0.0.1' /etc/resolv.conf > resolv.conf
cp resolv.conf /etc/resolv.conf
rm resolv.conf

/etc/init.d/bind9 restart
```

Script per configurar el servei ssh en client i servidor:

inici_ssh.sh

```
#!/bin/bash
function display_help(){
    echo -e "This script configurates ssh service in a indicated machine. All
machines
will install and configure openssh-server.
    Argument one: [server|router|client]
    "
}

while getopts :h option
do
 case "$option" in
    h)
       display_help
       exit 1
    ;;
     *)
       echo "ERROR: Invalid parameters" >&2
       display_help
       exit 1
    ;;
 esac
done

apt-get update # actualitzem repositoris sino de vegades dona error
apt-get install openssh-server

case "$1" in
    router)
       exit 0
```

```
        ;;
    server)
        exit 0
        ;;
    client)
      apt-get install openssh-client
        exit 0
        ;;
    *)
        echo -e "ERROR: machine indication needed:\n\trouter\n\tserver\n\tclient"
        exit 1
esac
```

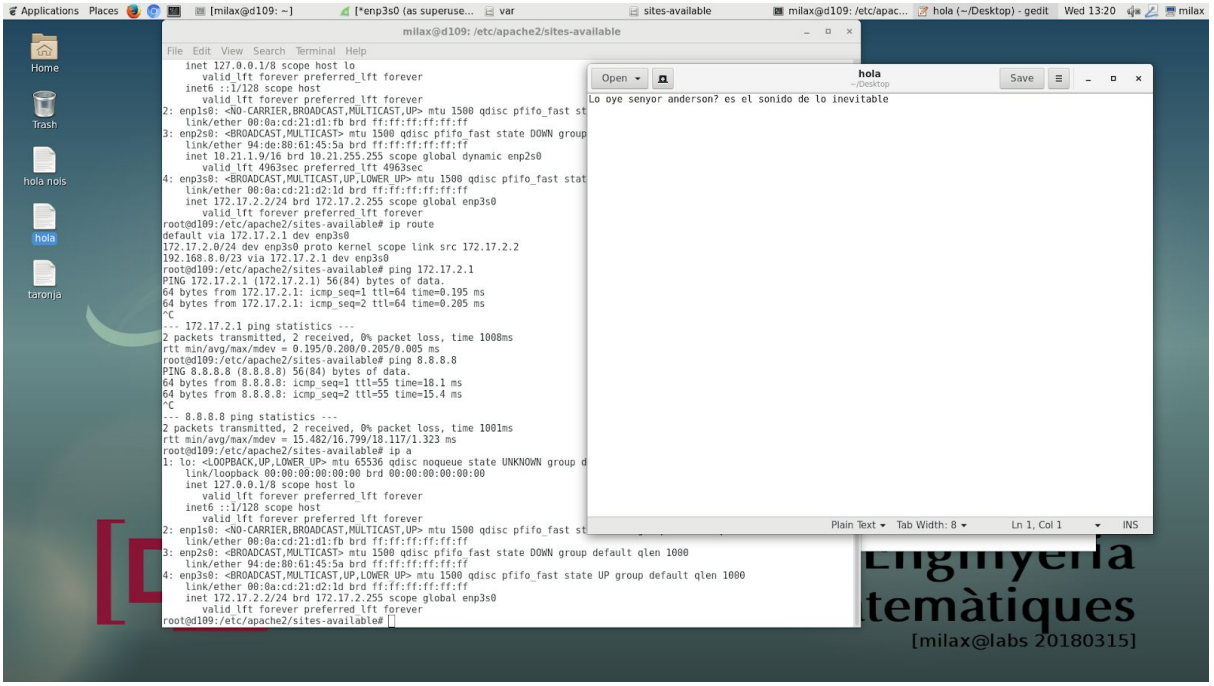
Ens connectem des del client al servidor mitjançant la comada (ssh usuari@host):
ssh server@www.tenda.grup2.gsx

Joc de Proves

Es pot dur a terme una connexió ssh des d'un ordinador extern a la xarxa, al servidor intern. Escribim en la carpeta d'usuari i en l'escriptori del servidor diversos missatges en diferents fitxers de pràctiques.

```
root@d100:/home/milax# ssh milax@www.tenda.grup2.gsx
milax@www.tenda.grup2.gsx's password:
Linux d109 4.9.0-6-amd64 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May 23 13:18:00 2018 from 10.21.1.0
milax@d109:~$ echo "Lo oye senyor anderson? es el sonido de lo inevitable" > matrix
milax@d109:~$ xmessage -buttons socunpringat:0 -default socunpringat -nearmouse "hola toful, carretonet del meu
corasonet" -timeout 100
```

S'observen els fitxers en el servidor creats per la màquina externa a la xarxa.


Applications Places
[milax@d109: ~]
[*enp3s0 (as superuse...
var
sites-available
milax@d109: /etc/apac...
hola (~/Desktop) - gedit
Wed 13:20
milax
Home
Trash
hola nois
hola
taronja
milax@d109: /etc/apache2/sites-available
File Edit View Search Terminal Help
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp1s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast st
link/ether 00:0a:cd:21:d1:fb brd ff:ff:ff:ff:ff:ff
3: enp2s0: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN group
link/ether 94:de:80:61:45:5a brd ff:ff:ff:ff:ff:ff
inet 10.21.1.9/16 brd 10.21.255.255 scope global dynamic enp2s0
valid_lft 4963sec preferred_lft 4963sec
4: enp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast stat
link/ether 00:0a:cd:21:d2:1d brd ff:ff:ff:ff:ff:ff
inet 172.17.2.2/24 brd 172.17.2.255 scope global enp3s0
valid_lft forever preferred_lft forever
root@d109:/etc/apache2/sites-available# ip route
default via 172.17.2.1 dev enp3s0
172.17.2.0/24 dev enp3s0 proto kernel scope link src 172.17.2.2
192.168.8.0/23 via 172.17.2.1 dev enp3s0
root@d109:/etc/apache2/sites-available# ping 172.17.2.1
PING 172.17.2.1 (172.17.2.1) 56(84) bytes of data.
64 bytes from 172.17.2.1: icmp_seq=1 ttl=64 time=0.195 ms
64 bytes from 172.17.2.1: icmp_seq=2 ttl=64 time=0.205 ms
^C
--- 172.17.2.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 0.195/0.200/0.205/0.005 ms
root@d109:/etc/apache2/sites-available# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=55 time=18.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=55 time=15.4 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 15.482/16.799/18.117/1.323 ms
root@d109:/etc/apache2/sites-available# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group d
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
valid_lft forever preferred_lft forever
2: enp1s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast st
link/ether 00:0a:cd:21:d1:fb brd ff:ff:ff:ff:ff:ff
3: enp2s0: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
link/ether 94:de:80:61:45:5a brd ff:ff:ff:ff:ff:ff
4: enp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 00:0a:cd:21:d2:1d brd ff:ff:ff:ff:ff:ff
inet 172.17.2.2/24 brd 172.17.2.255 scope global enp3s0
valid_lft forever preferred_lft forever
root@d109:/etc/apache2/sites-available#
Open
hola
~/Desktop
Save
Lo oye senyor anderson? es el sonido de lo inevitable
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
Enginyeria
temàtiques
[milax@labs 20180315]

Configuració del tallafocs:

El següent script configura les iptables per establir les regles del Firewall en les tres màquines:

firewall.sh

```
#!/bin/bash
function display_help(){
      echo -e "This script is for setting up the GSX firewall  configuration.
You have to indicate which machine do you want to configure in the first
argument:
\trouter\n\tclient\n\tserver
      "
}

function router_firewall(){
    #S'eliminen les regles anteriors
      iptables -F
      iptables -X
      iptables -t nat -F
      iptables -t nat -X

      iptables -P INPUT DROP
      iptables -P OUTPUT ACCEPT
      iptables -P FORWARD DROP

     #Es permet la resposta de les conexions establertes, configruacio
statefull

      iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

      iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
      iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
      iptables -A INPUT -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT

      #Es permet la comunicació de la màquina amb si mateixa.
      iptables -A INPUT -i lo -j ACCEPT
      iptables -A OUTPUT -o lo -j ACCEPT

      #Implementa SNAT quan la connexió prové d'una màquina de la xarxa
interna.
      iptables -t nat -A POSTROUTING -s 192.168.8.0/23 -j SNAT --to $addres
      iptables -t nat -A POSTROUTING -s 172.17.2.0/24 -j SNAT --to $addres
      iptables -t nat -A PREROUTING -i $i1 -p tcp --dport 80 -j DNAT
--to-destination 172.17.2.2:80
      iptables -t nat -A PREROUTING -i $i1 -p tcp --dport 443 -j DNAT
--to-destination 172.17.2.2:443
      iptables -t nat -A PREROUTING -i $i1 -p tcp --dport 23 -j DNAT
--to-destination 172.17.2.2:22


      #Permet el pas de les consultes DNS si van dirigides a un DNS
      iptables -A FORWARD -p udp  --dport 53 -j ACCEPT
```

```
      #Permet el pas de les comunicacions HTTP i HTTPS dirigides al Server de
la DMZ.
      iptables -A FORWARD -p tcp --dport 80 -j ACCEPT
      iptables -A FORWARD -p tcp --dport 443 -j ACCEPT

      #Permet sortir les comunicacions TCP que provenen d'una màquina de la
xarxa interna o de la DMZ.
      iptables -A FORWARD -p tcp -s 192.168.8.0/23 -j ACCEPT
      iptables -A FORWARD -p tcp -s 172.17.2.0/24 -j ACCEPT

}

function intranet_firewall(){
    #S'eliminen les regles anteriors
    iptables -F
      iptables -X

      iptables -P INPUT DROP
      iptables -P OUTPUT ACCEPT
      iptables -P FORWARD DROP

      iptables -A INPUT -i lo -j ACCEPT

      iptables -A INPUT -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT
      iptables -A INPUT -p udp -m state --state ESTABLISHED,RELATED -j ACCEPT
      iptables -A INPUT -p icmp -m state --state ESTABLISHED,RELATED -j ACCEPT

      #Accepta peticions de connexions SSH i/o SFTP.
      iptables -A INPUT -p tcp --dport 22 -j ACCEPT

      #Accepta i respon els "ping" des de qualsevol màquina de la xarxa
interna i/o la DMZ.
      iptables -A INPUT -p icmp --icmp-type 8 -s 192.168.8.0/24 -j ACCEPT
      iptables -A INPUT -p icmp --icmp-type 8 -s 172.17.2.0/24 -j ACCEPT

}

function dmz_firewall(){
    #S'eliminen les regles anteriors
    iptables -F
      iptables -X

      iptables -P INPUT DROP
      iptables -P OUTPUT DROP
      iptables -P FORWARD DROP

      iptables -A INPUT -i lo -j ACCEPT
      iptables -A OUTPUT -o lo -j ACCEPT

      #Es permet la resposta a peticions entrants
      iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

      #Accepta connexions SSH.
      iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

```
      #Accepta connexions HTTP i HTTPS.
      iptables -A INPUT -p tcp --dport 80 -j ACCEPT
      iptables -A INPUT -p tcp --dport 443 -j ACCEPT

      #Pot fer consultes DNS
      iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
      iptables -A INPUT -p udp -m state --state ESTABLISHED,RELATED -j ACCEPT

      iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT

      iptables -A INPUT -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT

      #Accepta i respon els "ping".
      iptables -A INPUT -p icmp --icmp-type 8 -j ACCEPT
      iptables -A OUTPUT -p icmp --icmp-type 8 -j ACCEPT


}


while getopts :h option
do
      case "$option" in
      h)
            display_help
            exit 1
      ;;
      *)
            echo "ERROR: Invalid parameters" >&2
            display_help
            exit 1
      ;;
  esac
done

case "$1" in
      router)
      router_firewall
      exit 0
      ;;
      client)
      intranet_firewall
      exit 0
      ;;
      server)
      dmz_firewall
      exit 0
      ;;
      *)
      echo -e "ERROR: machine indication needed:\n\trouter\n\tclient\n\tserver"
      exit 1
esac
```

Lab Servei Web Apache

Objectiu:

Preparar el servidor de la DMZ per a que serveixi a varis llocs web, configurant el servidor web apache. Posteriorment es realitza gestió d'Apache incrementant la seguretat del servidor web.

Decisions de disseny:

Configurarem un lloc web per defecte on hi hagi un missatge d'error a l'arrel.
Configurarem 2 llocs web Name-Based (taller i tenda).
Configurarem 1 lloc web IP-Based (serveis.intranet), per a l'accés des de la intranet.

Configuració:

El següent Script recopila copia tota l'estructura de contingut i configuració d'un servidor apache en un arxiu comprimit .tgz.

guarda_web.sh

```
#!/bin/bash

#Crea els directoris separant el contingut propi del web del de config Apache
mkdir websites
mkdir websites/html
mkdir websites/apache

#Copia el contingut html i les configuracions
cp -p /var/www/html ./websites/html
cp -p /etc/apache2/sites-available ./websites/apache

#Comprimeix els fitxers en format tgz
tar -cvzf websites.tgz ./websites
```

S'executa en el *Servidor* DMZ el següent script, el qual copia cada fitxer de configuració i codi html al directori corresponent i habilitar els nous serveis web, tot reactivant Apache:

inici_dmz_v3.sh

```
#!/bin/bash

#Copia el contingut html al directori corresponent
cp -p websites/html /var/www/html

#Copia els fitxers de configuració dels virtual hosts al directori conf Apache
cp -p websites/apache /etc/apache2/sites-available

#Habilita els virtual hosts
cd /etc/apache2/sites-available
```

```
a2ensite taller.conf
a2ensite tenda.conf

#Reinicia el servei apache
service apache2 restart
```

Els fitxers de codi HTML tenen el següent contingut:

index.html

```
<html>
  <head>
      <title>Index</title>
  </head>
  <body>
      <h1>ERROR! You souldn't be here!!!</h1>
  </body>
</html>
```

taller.html

```
<html>
  <head>
      <title>Taller</title>
  </head>
  <body>
      <h1>Hello to Taller</h1>
      <h1>This is the oficial taller Web Page!</h1>
  </body>
</html>
```

tenda.html

```
<html>
  <head>
      <title>Tenda</title>
  </head>
  <body>
      <h1>Hello to Tenda</h1>
      <h1>This is the oficial Tenda Web Page!</h1>
  </body>
</html>
```

Els fitxers de configuració dels virtual hosts són:

taller.conf

```
NameVirtualHost *:80
<VirtualHost *:80>
      ServerName www.taller.grup2.gsx
      ServerAlias *.taller.grup2.gsx *.taller
      DocumentRoot /var/www/html/taller
</VirtualHost>
```

tenda.conf

```
NameVirtualHost *:80
<VirtualHost *:80>
      ServerName www.tenda.grup2.gsx
      ServerAlias *.tenda.grup2.gsx *.tenda
      DocumentRoot /var/www/html/tenda
</VirtualHost>
```

Gestió amb Apache

Restringim l'accés al site de taller mitjançant **.htaccess** i **.htpasswd.**

S'executa l'script següent el qual crea la carpeta admin i afegeix el fitxer .htacces.

htaccess.sh

```
#!/bin/bash

#Crea la carpeta d'aministracio i afegeix el fitxer .htacces
mkdir /var/www/html/taller/admin
cp -p ./admin/taller_htaccess /var/www/html/taller/admin/.htaccess

#Reinicia el servei apache
service apache2 restart
```

A continuació es mostren els fitxers de gestió de la seguretat del site.
S'edita la configuració del site **taller.conf**, incloent la crida al directori **admin** el qual contindrà el fitxer **.htaccess** el qual contindra les configuracions de seguretat direccionant el fitxer **htpasswd**.

taller.conf

```
NameVirtualHost *:80
<VirtualHost *:80>
      ServerName www.taller.grup2.gsx
      ServerAlias *.taller.grup2.gsx *.taller
      DocumentRoot /var/www/html/taller
     #S'afegeix l'especificació següent per a la gestió amb contrasenya.
      <Directory "/var/www/html/taller/admin">
               Options Includes
               AllowOverride All
      </Directory>
</VirtualHost>
```

taller_htaccess

```
#Per protegir l'accés general a tot el site

AuthType Basic
AuthName "Zona Privada. Si us plau introduiu el password."
AuthUserFile "/var/www/html/taller/admin/.htpasswd"
Require valid-user

#Per protegir un fitxer concret

<FilesMatch "guarda_web.sh">

AuthType Basic
AuthName "Zona Privada. Si us plau introduiu el password."
AuthUserFile "/var/www/html/taller/admin/.htpasswd"
Require valid-user

</FilesMatch>
```

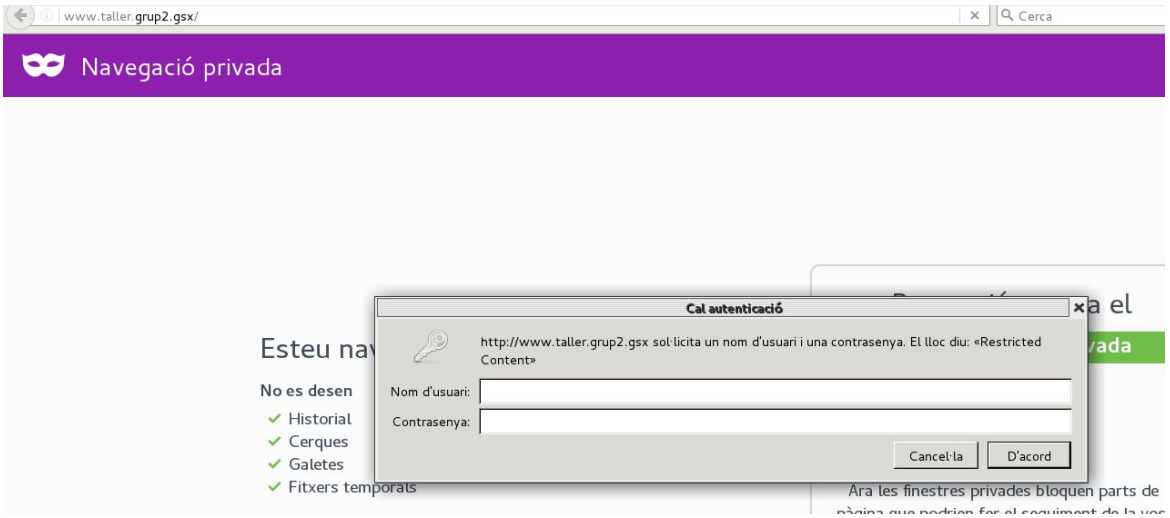
Finalment s'executa la comanda `htpasswd` per generar el fitxer `.htpasswd` creant un usuari i contrasenya encriptats. D'aquesta manera el servidor requerira de contrasenya a l'accedir al domini www .taller.grup2.gsx.cat per a mostrar el contingut web.
Es necessari fer-ho des del terminal ja que la contrasenya no es pot passar com argument des d'un script. S'ha de tenir instalat el paquet `apache2-utils`, per generar el fitxer encriptat de contrasenya, que es pot obtenir mitjançant `apt-get`.
S'ha assignat com a usuari *admin* i com a contrasenya *nimda*.

```
sudo htpasswd -c /var/www/html/taller/admin/.htpasswd admin
```

Joc de Proves

Aquestes captures han estat realitzades en el sistema de màquines virtuals, això mateix també s'ha provat en les maquines del laboratori accedint des de la màquina del professor a al servidor de la DMZ.
Accedim directament amb la ip del servidor:

Ara intentem accedir amb el nom de domini www.taller.grup2.gsx on ens demana autenticació:



Si introduïm correctament les credencials es mostra la plana web (admin i nimda):

En canvi, si ens equivoquem apareix la següent plana:

Finalment accedim a la tenda amb el domini www.tenda.grup2.gsx on no ens demana cap tipus d'autenticació.