PRACTICA No.17

"IP MASQUERADE"

OBJETIVO: La manera de construir una red con direcciones IP reservadas conectadas al Internet usando una maquina con Linux y que tenga 2 dispositivos de red (ya sea tarjetas de red, modem, etc.).

INTRODUCCIÓN:

En el mundo de las comunicaciones y de la computación tener varias plataformas (ejemplo : Windows, Novell, Unix, Linux, OS/2, VAX, Amiga, MacOs, etc.) en las computadoras y teniendo en cuenta que dichos sistemas operativos son expuestos a los ataques de intrusos y estos pueden usar recursos y/o destruir la información de las máquinas atacadas. Por otro lado, uno de los problemas que enfrenta actualmente Internet es la escasez de direcciones IP ya que día con día se conectan más computadoras a la red mundial para la conseguir información, comercio electrónico, etc. por lo que una manera fácil de resolver estos problemas es la implementación de un IP masquerade utilizando una computadora con sistema operativo Linux, ya que con esto podemos conectar redes LAN usando dirección IP reservadas ó sin clase y las maquinas alojadas tengan un acceso invisible al Internet y no están expuestas contra los intrusos, además se ahorra un número considerable de direcciones IP, ya que solamente se usará la IP oficial la maquina que se utilizará como gateway.

DESARROLLO:

Nuestra computadora con Linux hará su función de gateway y su respectiva labor de filtrado de paquetes provenientes de Internet. Para entender un poco de donde se puede usar direcciones IP reservadas ó sin clase, veremos como están distribuidas estas mismas.

Cada host y enrutador de Internet tiene una dirección IP, que codifica sin número de red y su número de host. La combinación es única ; no hay 2 máquinas que tengan la misma dirección IP. Todas las direcciones de IP son de 32 bits de longitud y se usan en los campos de dirección origen y de dirección destino. Donde hay 3 clases principales de dirección : A, B y C.

En una dirección de clase A, el primer byte representa la porción de red y los otros 3 identifican al host. Esto significan que la red puede tener millones de hosts, debido a que se dispone de 24 bits para identificar la dirección del host. De hecho, la dirección 0.0.0.0 (conocido como el ruteo por default) y 127.0.0.0 (la red de retorno de lazo) tiene un especial significado y no están disponibles para su identificación de la red. Así estas son únicamente de la dirección 126 que esta disponible a la clase A.

La dirección de clase B tiene16 bits para la red y otros 16 para el host. El rango de la clase B va de la 128 a la 191, cada red contiene arriba de 32766 posibles interfases.

La clase C tiene 24bits para la red y 8 para el host, la cual tiene un rango de 192 a 254. Estas así son 4,194,303 disponibles números de red de la clase C, cada red contiene 254 interfases.

También existen unas direcciones especiales que están reservadas para la "no conexión" en la Internet, esta direcciones son :

1. Una red Clase A :
   10.0.0.0
2. 16 redes Clase B :
   172.16.0.0 - 172.31.0.0
3. 256 redes Clase C :
   192.168.0.0 - 192.168.255.0

x.x.x.0 Que identifica a toda la red.

x.x.x.255 Identifica a todos los host de la red especificada.

Todas las direcciones de difusión de host para todas las redes actuales.

También existe la mascara de red, con ellas se puede hacer saber si es una red de tipo A, B, C o si queremos que una clase tipo C se divida en subredes, con el movimiento de bits en la mascara de red podemos dividirlo.

La mascara de red standard es todos los bits de red en una dirección puesta a 1 y todos los bits del host puesta a 0. Estos son los estandares de las mascara de red de las 3 clases :

Clase A mascara de red : 255.0.0.0

Clase B mascara de red : 255.255.0.0

Clase C mascara de red : 255.255.255.0

Clase D mascara de red : 255.255.255.255

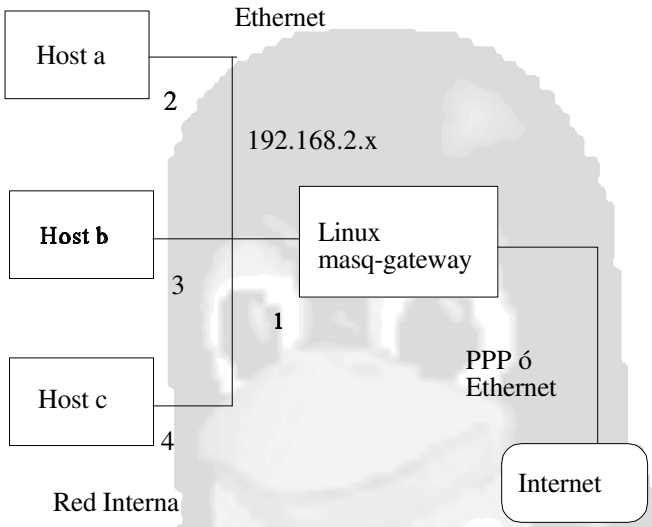
Ahora veremos la aplicación de las subredes con movimiento de los bits en la mascara de red y se tiene un ejemplo :

No. de Subred	No. de host en la red	Mascara de red
2	126	255.255.255.128
4	62	255.255.255.192
8	30	255.255.255.224
16	14	255.255.255.240
32	6	255.255.255.248
64	2	255.255.255.252

Otra manera de ver la división de la subred es las siguiente :

Mascara de Red	subred	Red	Broadcast	min. IP	Máx. IP	Host	Total Host
128	2	0	127	1	126	126	
		128	255	129	254	126	252
192	4	0	63	1	62	62	
		64	127	65	126	62	
		128	191	129	190	62	
		192	255	193	254	62	248
224	8	0	31	1	30	30	
		32	63	33	62	30	
		64	95	65	94	30	
		96	127	97	126	30	
		128	159	129	158	30	
		160	191	161	190	30	
		192	223	193	222	30	
		224	255	225	254	30	240

Ahora daremos un ejemplo de la forma de conexión que se pretende hacer. Aquí se abarca que se tiene una red interna con una variedad de sistemas operativos y que todas esas computadoras quieren usar Navegadores WEB, ftp, telnet, Real Audio, IRC, etc.



Como se puede observar tenemos una red interna y que puede tener cualquier sistema operativo (Windows9x/NT, Windows 3.11, Novell, Unix, Macintosh MacTCP, Linux, etc.) donde se ve que se usa una red clase tipo C (192.168.2.0) y el host con Linux tiene una dirección con la dirección 192.168.2.1 y tiene otra dirección que es reconocida por la red mundial, además está maquina tiene un sistema masq-gateway que convierte toda estas conexiones y tiene la capacidad de pasar la información para las maquinas de la Internet con la red interna y la distribución de la información. Como se puede observar el kernel de Linux tiene un mecanismo del uso de un firewall : masquerade de paquetes IP. Así, la dirección IP fuente es reemplazada por la dirección IP local y el puerto fuente es reemplazado por un puerto local. Comenzando una administración guardada de sesiones enmascaradas (masqueraded), después los paquetes que regresan de los puertos será automáticamente serán “desenmascarados” y mandados al sistema que originalmente hizo la petición :

Una forma más clara es usando una tabla con los sig. valores :

Queremos hacer una conexión telnet (puerto 23), de la maquina 192.168.2.2 (maquina Interna), a la maquina 132.248.52.191 (maquina Externa), pasando por un sistema Linux enmascarado (masquerading) con IP 192.168.2.1-132.248.59.142

	Fuente		Destino	
	Dirección IP	puerto	Dirección IP	Puerto
paquete original	192.168.2.2	1027	132.248.52.191	23
enmascarar	192.168.2.1/132.248.59.142	32545	132.248.52.191	23
paquete retornado	132.248.52.191	23	192.168.2.1/132.248.59.142	32545
desenmascarar	132.248.52.191	23	192.168.2.2	1027

Aquí hay un detalle muy importante, como está haciendo el intercambio de paquetes una maquina que tiene como dirección IP una de las reservadas para no tener conexión y se la pueda mandar a otra que si tiene conexión al exterior. Esto se ve muy simple si recordamos que en una maquina con Linux se tienen que poner 2 tarjetas de red ó 2 conexiones con modem o la combinación de ambos, una de esta conexión estará con la red interna y la otra con la externa, mientras que el kernel de Linux tiene programas que hace el intercambio de paquetes entre las 2 tarjetas y todo es transparente, claro que se tienen que hacer una serie de pasos para obtener la configuración deseada, pero con ello logramos 3 cosas muy importantes :

I. Proteger de Intrusos a la red interna.
I I . Ahorrar direcciones IP y distribuirlas a otras redes de mayor importancia ó implementar otros masquerade.
III. Administrar y monitorear las conexiones de los usuarios, ya que con esto sabemos a que maquina se conecta, con que protocolo y cuanto dura su conexión.

1)Configurar las 2 tarjetas de red, o conexión por módem (en este caso manejaremos 2 tarjetas, para la congruencia del texto).

2)Recompilar el kernel con las opciones de soporte para:

```
#make menuconfig

*Buscar las 2 tarjetas correpondientes para tener sus drivers.
```

*Prompt for development and/or incomplete code/drivers
CONFIG_EXPERIMENTAL
-this will allow you select experimental ip_masq code compiled into the kernel.

*Enable loadable module support
CONFIG_MODULES
-allows you to load modules

*Networking support
CONFIG_NET

*Network firewalls
CONFIG_NET

*TCP/IP networking
CONFIG_INET

*IP: forwarding/gatewaying
CONFIG_IP_FORWARD

*IP: firewalling
CONFIG_IP_FIREWALL

*IP: masqueradinf (EXPERIMENTAL)
CONFIG_IP_MASQUERADE
-although it is experimental, it is a “MUST”

*IP: always defragment
CONFIG_IP_ALWAYS_DEFRAG
-highly recommended

*Dummy net driver support
CONFIG_DUMMY
-recommended

Después de compilar el kernel, también compilaremos e instalaremos los modulos:

```
#make modules ; make modules_install
```

Mientras compila el kernel y modulos podemos configurar la nueva interfaz, copiando el archivo /etc/sysconfig/network-scripts/ifcfg-eth0:

```
# c p     /e t c / s y s c o n f i g / n e t w o r k - s c r i p t s / i f c f g - e t h 0
/etc/sysconfig/network-scripts/ifcfg-eth1
```

Ahora lo modificaremos para soportar la red interna, quedando de esta manera:

```
#vi /etc/sysconfig/network-scripts/ifcfg-eth1
```

```
DEVICE=eth1
IPADDR=192.168.2.1
NETWORK=192.168.2.0
NETMASK=255.255.255.0
BROADCAST=192.168.2.255
ONBOOT=yes
BOOTPROTO=none
```

También cargaremos los módulos cada vez que inicie la maquina los paquetes del conocido ipv4 (ejemplos : ip_masq_ftp, ip_masq_raudio, ip_masq_irc, etc.). Para que podamos usar esos servicios en forma transparente, podemos poner estas líneas en el archivo /etc/rc.d/rc.local y se ejecutará cada vez que se inicie la maquina:

```
#vi /etc/rc.d/rc.local

      .
      .
      .
/sbin/depmod -a
/sbin/modprobe ip_masq_ftp
/sbin/modprobe ip_masq_raudio
/sbin/modprobe ip_masq_irc
```

Salvamos el archivo.

Acabando de recompilar el kernel, reiniciar la computadora, se tendrá que reconocer las 2 tarjetas, los modulos y posteriormente se dirá a una de ellas que va estar en una red interna y la otra a la red mundial.

Nota: Para ver si reconoce las tarjetas use el comando dmesg, para la configuración de las tarjetas de red use ifconfig, para los modulos lsmod o ver el archivo /var/log/messages

```
#dmesg
      .
      .
      .
      .
PPP Dynamic channel allocation code copyright 1995 Caldera, Inc.PPP line discipline registered.
tulip.c:v0.88 4/7/98 becker@cesdis.gsfc.nasa.gov
eth0: Digital DS21142/3 Tulip at 0x6100, 00 48 54 00 24 61, IRQ 11.
eth0:  EEPROM default media type Autosense.
eth0:  Index #0 - Media 10baseT (#0) described by a 21142 Serial PHY (2) block.
eth0:  Index #1 - Media 10baseT-FD (#4) described by a 21142 Serial PHY (2) block.
eth0:  Index #2 - Media 100baseTx (#3) described by a 21143 SYM PHY (4) block.
eth0:  Index #3 - Media 100baseTx-FD (#5) described by a 21143 SYM PHY (4) block.
```

```
eth1: 3c509 at 0x300 tag 1, BNC port, address 00 a0 24 2f 30 69, IRQ 10
3c509.c:1.07  6/15/95 becker@cesdis.gsfc.nasa.gov
Partition check:
      .
      .
```

```
#ifconfig

lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Bcast:127.255.255.255 Mask:255.0.0.0
      UP BROADCAST LOOPBACK RUNNING MTU:3584  Metric: 1
      RX packets:307 errors:0 dropped:0 overruns:0
      TX packets:7   errors:0 dropped:0 overruns:0

eth0  Link encap:Ethernet Hwaddr 00:48:54:00:24:61
      inet addr:132.248.59.66 Bcast:132.248.59.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric: 1
      RX packets:1546 errors:2 dropped:0 overruns:0
      TX packets:2347 errors:0 dropped:0 overruns:0
      Interrupt:11   Base Address: 0x6100



eth1  Link encap:Ethernet Hwaddr 00:A0:24:2F:30:69
      inet addr:192.168.2.1 Bcast:192.168.2.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric: 1
      RX packets:2034 errors:2 dropped:0 overruns:0
      TX packets:12247 errors:0 dropped:0 overruns:0
      Interrupt:10   Base Address:0x300
```

```
#lsmod

Module         Pages    Used by
ip_masq_raudio     1          0
ip_masq_ftp        1          0
ip_masq_irc        1          0
sb                 6          0
uart401            2    [sb]  0
sound             16    [sb uart401]      0
```

Ahora se hará la configuración de las maquinas dentro de la red virtual de los siguientes sistemas operativos :

Windows9x.- Después de instalar la tarjeta y que la reconociera, ir al “panel de control/red”, agregando el “protocolo de TCP/IP”.

En “TCP/IP propiedades”, colocar en “IP Address” y poner la dirección IP del rango 192.168.2.x (1<x<255) y la mascara de subred de 255.255.255.0. Agregando 192.168.2.1 como tu gateway en la opción de “gateway”.

Después se agregará en la "Configuración del DNS/DNS Server search order" poner un DNS conocido.

Acabando de configurar estos cambios reiniciar la maquina correspondiente y podemos checar si tu maquina ve al servidor Linux, usando el comando ping en la parte de "Ejecutar" pondremos : ping 192.168.2.1. Si reponde nuestra maquina llevamos una gran parte de la configuración.

Windows for Workgroup 3.11.- Aqui hay 2 formas para configurar:

- Instalar el paquete de TCP/IP 32b, posteriormente en "Main/Windows setup/Network setup", dar un click en "Drivers". Poner la dirección IP 192.168.2.x (1<x<255), tambien la sured de 255.255.255.0 y default gateway 192.168.2.1.

- Vemos que los drivers de la tarjetas y emuladores estén configurados (winpkt), posteriormente en el autoexec.bat se pondrá la sintaxis set ip= 192.168.2.x. (1<x<255) Ahora en el programa Trumpet Winsock en el setup se pondrán los siguientes valores :

  IP Address 192.168.2.x (1<x<255)
  Netmask 255.255.255.0
  Domain Name Server
  Default Gateway 192.168.2.1

Reinicie el Trumpet y estará los nuevos valores de configuración.

Windows NT 4.0.- Nos vamos al panel de control, seleccionamos red, posteriormente vemos el modulo de protocolos y seleccionamos la configuración de TCP/IP e introducimos los valores :
dirección IP 192.168.2.x (1<x<255)
netmask 255.255.255.0.
Gateway 192.168.2.1

Configuración de Sistemas UNIX.- Si no tienes una tarjeta de red, tienes que configurarla recompilando el kernel, posteriormente instalas las utilerías de TCP/IP. dirección IP 192.168.2.x (1<x<255), Gateway 192.168.2.1 y netsmak 255.255.255.0 como también el BRADCAST 192.168.2.255. Un ejemplo de Linux redhat está en el archivo /etc/sysconfig/network-scripts/ifcfg-eth0. Agregas el DNS en el archivo /etc/resolv.conf, actualiza el archivo /etc/networks, restaura tus servicios o simplemente restaura tu computadora.

Usa el comando ping : ping 192.168.2.1 y observa si tu gateway está funcionando.

Nuestra maquina Linux usará el programa de ruteo entre las 2 tarjetas para que haga una función de gateway, llamado este programa en Linux ipfwadm (ip-firewall-administrator), aunque se tiene una segunda opción usando el comando ipchains.

Las políticas de IP Forwarding de la opción ipfwadm y teniendo en orden tanto el kernel, las tarjetas y módulos. Ahora necesitamos el gateway real, DNS, para la maquina Linux.

Ahora, las opciones de ipfwadm para mandar los paquetes apropiados en la maquina gateway :

#ipfwadm -F -p deny
#ipfwadm -F -a m -S yyy.yyy.yyy.yyy/x -D 0.0.0.0/0

Con ipchains :

#ipchains -P forward DENY
#ipchains -A forwa rd -j MASQ -s yyy.yyy.yyy.yyy/x -d 0.0.0.0/0

Donde x es uno de los siguientes números de acuerdo a la clase de subred y la dirección de la red es yyy.yyy.yyy.yyy :

Mascara de red	x	Subred
255.0.0.0	8	Clase Tipo A
255.255.0.0	16	Clase Tipo B
255.255.255.0	24	Clase Tipo C
255.255.255.255	32	Punto a Punto

Un ejemplo a esta aplicación será (el que usarmeos para está practica):

```
#ipfwadm -F -p deny

#ipfwadm -F -a m -S 192.168.2.0/24  -D  0.0.0.0/0
```

Con ipchains :

#ipchains -P forward DENY
#ipchains -A forward -j MASQ -s 192.168.2.0/24 -d 0.0.0.0/0

En el ejemplo se observa que rutea la red tipo C (192.168.2.0) y no le importa a que puerto se conecte a la salida de la tarjeta de red (0.0.0.0). Para que no estemos poniendo los comandos cada vez que inicie la maquina, los pondremos ponerlo en un archivo (ejemplo: /etc/rc.d/rc.local) para que se inicien.

Una de las virtudes de este comando ipfwadm es la posibilidad de rutear maquinas punto a punto (de manera individual). En el sig. ejemplo solamente tendrá acceso a Internet las maquinas con IP 192.168.2.4 y 192.168.2.5 :

```
#ipfwadm -F  -p deny

#ipfwadm -F  -a m -S 192.168.2.4/32  -D  0.0.0.0/0

#ipfwadm -F  -a m -S 192.168.2.5/32  -D  0.0.0.0/0
```

Con ipchains :

```
#ipchains -P forward DENY

#ipchains -A forward -j MASQ -s 192.168.2.4/32  -d 0.0.0.0/0

#ipchains -A forward -j MASQ -s 192.168.2.5/32  -d 0.0.0.0/0
```

Para observar las diferentes conexiones de las maquinas clientes se puede utilizar la opción de :

```
#ipfwadm -M -l
```

Con ipchains :

```
#ipfwadm -M -L
```

Mostrando algo semejante :

```
IP masquerading entries
prot  expire     source          destination           ports
tcp   12 :25.1   192.168.2.6     www.unam.mx       1017 (80) ->http
tcp   14 :52.12 rush.comp.fi   cronos.fi-b.unam.mx 1345 (6023) ->telnet
```

Donde está información se encuentra en un pseudo-archivo que es leído y se llama /proc/net/ip_masquerade y que se puede leer por la conversión del ipfwadm. Con esto podemos conectar una red y que pueda utilizar Internet con una dirección IP, funcioanndo como gateway el host Linux.

CONCLUSIONES