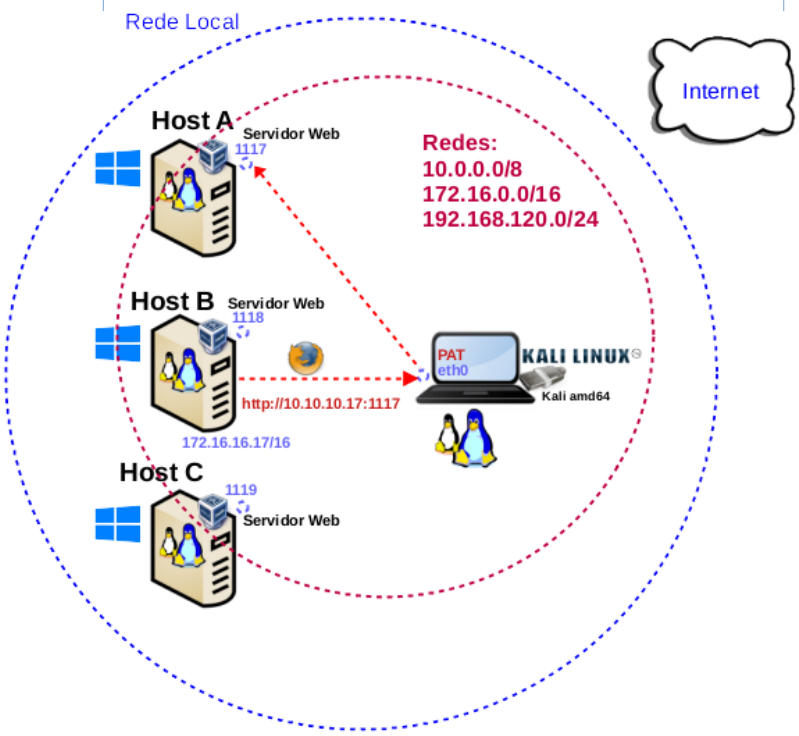
TALLER SR – PRÁCTICA 61 – PAT

NÚMERO DE GRUPO	FUNCIÓNS	Apelidos, Nome
	Coordinador/a:	
	Responsable Limpeza:	
	Responsable Documentación:	

ESCENARIO: PAT

Portátil:
Rede Local
MAC filtrada (sen acceso)
Firewall → iptables → DNAT
Rede1: 10.0.0.0/8
IP/MS: 10.10.10.200/8
Rede2: 172.16.0.0/16
IP/MS: 172.16.16.200/16
Rede3: 192.168.120.0/24
IP/MS: 192.168.120.200/24
echo 1 > /proc/sys/net/ipv4/ip_forward

USB
Live Kali amd64
Hosts A, B, C:
∈ Rede Local
⊃ Máquina virtual



Máquinas virtuais:
⊂ Host
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
Rede: Bridge
ISO: Kali Live amd64
Servidor Web: php -S IP:Port -t DocumentRoot/
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

Máquina virtual hostA:
Rede: 10.10.10.0/8
IP/MS: 10.10.10.XY
Gateway: 10.10.10.200
$ php -S 10.10.10.17:1117 -t web17

Máquina virtual hostB:
Rede2: 172.16.0.0/16
IP/MS: 172.16.16.XY/16
Gateway: 172.16.16.200
$ php -S 172.16.16.18:1118 -t web18

Máquina virtual hostC:
Rede: 192.168.120.0/24
IP/MS: 192.168.120.XY/16
Gateway: 192.168.120.200
$ php -S 192.168.120.19:1119 -t web19

Material necesario	Práctica: PAT
■ Portátil ■ Regleta ■ Switch 5-Port Gigabit ■ USB Live amd64 Kali ■ Hosts alumnado ■ Cableado de rede ■ [1] Práctica 1 ■ [2] Práctica SI Firewall iptables	(1) Prerrequisito: Ter realizada a Práctica 1 [1] (2) **NON conectar o switch á roseta da aula.** (3) Conectar o portátil e hosts alumnado ao switch. (4) Hosts alumnado: a) Crear máquinas virtuais coa rede en modo “Bridge” e especificacións según escenario. b) Arrancar máquina virtual. Configurar rede según escenario. c) Instalar/arrancar un servidor web (ver escenario). d) Xerar ficheiro identificativo da máquina virtual no DocumentRoot (5) Portátil: a) Configurar a rede según escenario. b) Regras iptables: redireccionar portos (DNAT). (6) Máquinas virtuais hosts alumnado: Peticións web que serán redireccionadas por PAT.

Procedemento:

(1) **Conectar no mesmo segmento de rede o portátil e os hosts do alumnado.**

(a) **NON conectar o switch á roseta da aula.**

(b) Conectar a regleta á corrente eléctrica na vosa zona de traballo.

(c) Conectar o switch á regleta.

(d) Conectar o portátil ao switch co cableado de rede creado na Práctica 1 [1] .

(e) Conectar os vosos equipos de alumnado ao switch.

(2) Hosts alumnado.

(a) Crear unha máquina virtual en cada equipo do alumnado coas seguintes características (ver escenario):

I. RAM ≥ 2048MB
II. CPU ≥ 2
III. PAE/NX habilitado
IV. Rede: Soamente unha tarxeta activada en modo bridge (ponte)
V. ISO: Kali Live amd64
VI. Nome: Practica61-PAT-AlumnoXY, *o valor XY é o valor do PC que tedes asignado. Así, o alumno 17 terá como nome da máquina virtual: Practica61-PAT-Alumno17*

(b) Arrancar máquina virtual.

(c) Configurar a rede para a NIC eth0 en cada máquina virtual según escenario. Así, executar nunha consola:

I. Para a máquina virtual pertencente ao hostA:

```
$ setxkbmap es #Configurar teclado en español

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

  # /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 conflicto con este demo.

  # /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.

  # ip addr show eth0 #Amosar información sobre a NIC eth0.

  # ip addr add 10.10.10.XY/8 dev eth0 #Substituír XY polo seu valor correspondente. O valor XY é o valor do PC que tedes asignado. Así, o alumno 17 terá que configurar a tarxeta de rede eth0, coa IP: 10.10.10.17 e máscara de subrede: 255.0.0.0

  # ip addr show eth0 #Amosar información sobre a NIC eth0.

  # exit #Saír da shell
```

II. Para a máquina virtual pertencente ao hostB:

```
$ setxkbmap es #Configurar teclado en español

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

  # /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 conflicto con este demo.

  # /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.

  # ip addr show eth0 #Amosar información sobre a NIC eth0.

  # ip addr add 172.16.16.XY/16 dev eth0 #Substituír XY polo seu valor correspondente. O valor XY é o valor do PC que tedes asignado. Así, o alumno 17 terá que configurar a tarxeta de rede eth0, coa IP: 172.16.16.17 e máscara de subrede: 255.255.0.0

  # ip addr show eth0 #Amosar información sobre a NIC eth0.

  # exit #Saír da shell
```

III. Para a máquina virtual pertencente ao hostC:

```
$ setxkbmap es #Configurar teclado en español

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

  # /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 conflicto con este demo.
```

```
# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.
# ip addr show eth0 #Amosar información sobre a NIC eth0.
# ip addr add 192.168.120.XY/24 dev eth0 #Substituír XY polo seu valor correspondente. O valor XY é o valor do PC que tedes asignado. Así, o alumno 17 terá que configurar a tarxeta de rede eth0, coa IP: 192.168.120.17 e máscara de subrede: 255.255.255.0
# ip addr show eth0 #Amosar información sobre a NIC eth0.
# exit #Saír da shell
```

(d) Configurar e activar un servidor web en cada máquina virtual anterior. Executar na consola correspondente:

NOTA: Lembrar substituír XY polo seu valor correspondente. O valor XY é o valor do PC que tedes asignado. Así, o alumno 17 terá que XY=17

```
$ mkdir webXY #Substituír XY polo seu valor correspondente. O valor XY é o valor do PC que tedes asignado. Así, o alumno 17 creará o cartafol web17
$ cat > webXY/index.php <<EOF #Xerar o ficheiro index.php
<?php
echo "<style>
.bgcyan{background-color:cyan;}
.bgsalmon{background-color:salmon;}
.bglime{background-color:lime;}
.bgsalmonminus{background-color:#fbaca3;}
.bggreenminus{background-color:#97fa97;}
</style>";
echo "<table border=1 cellspacing=0 cellpadding=2>";
echo "<tr><th colspan=2 class='bgcyan'>AlumnoXY</th></tr>";
echo "<tr><th class='bgsalmon'>SERVER</th><th class='bglime'>CLIENT</th></tr>";
echo "<tr>";
echo "<td class='bgsalmonminus'>".\$_SERVER['HTTP_HOST']."</td>";
echo "<td class='bggreenminus'>".\$_SERVER['REMOTE_ADDR'].":".\$_SERVER['REMOTE_PORT']."</td>";
echo "</tr>";
echo "</table>";
?>
EOF
```

I. Para a máquina virtual pertencente ao hostA:

```
$ php -S 10.10.10.XY:11XY -t ./webXY #Arrancar un servidor web en 10.10.10.XY no porto TCP 11XY, onde o DocumentRoot é o cartafol webXY.
```

II. Para a máquina virtual pertencente ao hostB:

```
$ php -S 172.16.16.XY:11XY -t ./webXY #Arrancar un servidor web en 172.16.16.XY no porto TCP 11XY, onde o DocumentRoot é o cartafol webXY.
```

III. Para a máquina virtual pertencente ao hostC:

```
$ php -S 192.168.120.XY:11XY -t ./webXY #Arrancar un servidor web en 192.168.120.XY no porto TCP 11XY, onde o DocumentRoot é o cartafol webXY.
```

(e) Abrir un navegador e visitar as URLs correspondentes ás 3 máquinas virtuais Practica61-PAT-AlumnoXY

I. Para a máquina virtual pertencente ao hostA. Visitar a URL: `http://10.10.10.XY:11XY`

II. Para a máquina virtual pertencente ao hostB. Visitar a URL: `http://172.16.16.XY:11XY`

III. Para a máquina virtual pertencente ao hostC. Visitar a URL: `http://192.168.120.XY:11XY`

(f) Dende cada máquina virtual visitar as 3 URLs anteriores. Que acontece? Por que?

(g) Avisar ao docente para a revisión. ☐

(3) Portátil:

(a) Arrancar co USB Live Kali amd64.

(b) Configurar a rede para a NIC eth0. Executar nunha consola:

```
$ setxkbmap es #Configurar teclado en español

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

  # /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 conflicto con este demo.

  # /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.

  # ip addr show eth0 #Amosar información sobre a NIC eth0.

  # ip addr add 10.10.10.200/8 dev eth0 #Configurar a tarxeta de rede eth0, coa IP: 10.10.10.200 e máscara de subrede: 255.0.0.0

  # ip addr add 172.16.16.200/16 dev eth0 #Configurar a tarxeta de rede eth0, coa IP: 172.16.16.200 e máscara de subrede: 255.255.0.0

  # ip addr add 192.168.120.200/24 dev eth0 #Configurar a tarxeta de rede eth0, coa IP: 192.168.120.200 e máscara de subrede: 255.255.255.0

  # ip addr show eth0 #Amosar información sobre a NIC eth0.
```

(4) Conectar no mesmo segmento de rede o portátil e os hosts do alumnado, é dicir, conectar os vosos equipos de alumnado ao switch.

(5) Portátil. Comprobar a conectividade de rede coa máquinas virtuais:

```
  # ping -c4 10.10.10.XY #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostA.

  # ping -c4 172.16.16.XY #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostB.

  # ping -c4 192.168.120.XY #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostC.
```

(6) Avisar ao docente para a revisión. ☐

(7) Máquinas virtuais dos hosts do alumnado: Configuración da porta de enlace por defecto. Executar noutra consola:

I. Para a máquina virtual pertencente ao hostA.

```
$ ip addr show #Amosar información sobre as NIC do sistema operativo.

$ ip route #Amosar a táboa de enrutamento.

$ cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, no cal configúranse os servidores DNS mediante a directiva nameserver.

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

  # ip route add default via 10.10.10.200 dev eth0 #Pór como porta de enlace 10.10.10.200 (a IP do portátil)

  # ip addr show #Amosar información sobre as NIC do sistema operativo..

  # ip route #Amosar a táboa de enrutamento.

  # cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, no cal configúranse os servidores DNS mediante a directiva nameserver.
```

II. Para a máquina virtual pertencente ao hostB:

```
$ ip addr show #Amosar información sobre as NIC do sistema operativo.

$ ip route #Amosar a táboa de enrutamento.

$ cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, no cal configúranse os servidores DNS mediante a directiva nameserver.

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

  # ip route add default via 172.16.16.200 dev eth0 #Pór como porta de enlace 172.16.16.200 (a IP do portátil)

  # ip addr show #Amosar información sobre as NIC do sistema operativo..

  # ip route #Amosar a táboa de enrutamento.

  # cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, no cal configúranse os servidores DNS mediante a directiva nameserver.
```

III. Para a máquina virtual pertencente ao hostC:

```
$ ip addr show #Amosar información sobre as NIC do sistema operativo.
$ ip route #Amosar a táboa de enrutamento.
$ cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, no cal configúranse os servidores DNS mediante a directiva nameserver.
$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
  # ip route add default via 192.168.120.200 dev eth0 #Pór como porta de enlace 192.168.120.200 (a IP do portátil)
  # ip addr show #Amosar información sobre as NIC do sistema operativo..
  # ip route #Amosar a táboa de enrutamento.
  # cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, no cal configúranse os servidores DNS mediante a directiva nameserver.
```

(b) Realizar de novo o apartado (2e). Indicar que acontece. Por que?

(c) Comprobar a conectividade de rede co portátil. Indicar que acontece. Por que?

I. Para a máquina virtual pertencente ao hostA.

```
# ping -c4 10.10.10.200 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostA.
# ping -c4 172.16.16.200 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostB.
# ping -c4 192.168.120.200 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostC.
```

II. Para a máquina virtual pertencente ao hostB.

```
# ping -c4 10.10.10.200 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostA.
# ping -c4 172.16.16.200 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostB.
# ping -c4 192.168.120.200 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostC.
```

III. Para a máquina virtual pertencente ao hostC.

```
# ping -c4 10.10.10.200 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostA.
# ping -c4 172.16.16.200 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostB.
# ping -c4 192.168.120.200 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostC.
```

(d) Avisar ao docente para a revisión. ☐

(8) Portátil. Regras iptables: redireccionar portos ás máquinas virtuais dos hosts do alumnado. Executar na anterior consola:

```
# iptables -F #Eliminar todas as regras de todas as cadeas da táboa filter.
# iptables -F -t nat #Eliminar todas as regras de todas as cadeas da táboa nat.
# iptables -L --line-numbers -t nat -v #Listar de forma numerada todas as regras das cadeas da táboa nat, é dicir, amosar de forma numerada todas as regras das cadeas PREROUTING, INPUT, POSTROUTING e OUTPUT. A opción -v é a opción versbose e amosa máis información, entre a que destaca a cantidade de bytes e paquetes que son afectados a cada regra, é dicir, sé unha regra non actúa no firewall terá valores nulos, polo contra, canto máis actúe máis valores terá.
# iptables -t nat -I PREROUTING -p tcp --dport 11XY -j DNAT --to-destination 10.10.10.XY:11XY #Redireccionar no portátil calquera chamada dende a rede ao porto TCP 11XY, correspondente ao porto TCP do servidor web da máquina virtual do hostA, á IP 10.10.10.XY no porto TCP 11XY
# iptables -t nat -I PREROUTING -p tcp --dport 11XY -j DNAT --to-destination 172.16.16.XY:11XY #Redireccionar no portátil calquera chamada dende a rede ao porto TCP 11XY, correspondente ao porto TCP do servidor web da máquina virtual do hostB, á IP 172.16.16.XY no porto TCP 11XY
# iptables -t nat -I PREROUTING -p tcp --dport 11XY -j DNAT --to-destination 192.168.120.XY:11XY #Redireccionar no portátil calquera chamada dende a rede ao porto TCP 11XY, correspondente ao porto TCP do servidor web da máquina virtual do hostC, á IP 172.16.16.XY no porto TCP 11XY
# iptables -L --line-numbers -t nat -v #Listar de forma numerada todas as regras das cadeas da táboa nat, é dicir, amosar de forma numerada todas as regras das cadeas PREROUTING, INPUT, POSTROUTING e OUTPUT. A opción -v é a opción versbose e amosa máis información, entre a que destaca a cantidade de bytes e paquetes que son afectados a cada regra, é dicir, se unha regra non actúa no firewall terá valores nulos, polo contra, canto máis actúe máis valores terá.
```

(9) Máquinas virtuais dos hosts do alumnado: Realizar de novo os apartado (2e) e (7c). Indicar que acontece. Por que?

(10) Portátil. Permitir o enrutamento entre interfaces de rede. Executar nunha consola:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward #Activar enrutamento entre interfaces, é dicir, permitir que pasen paquetes entre eth0(bridge) e eth1(rede interna)
```

(a) Realizar de novo os apartados (2e) e (7c). Indicar que acontece. Por que?

(b) Avisar ao docente para revisión. ☐

(11) Razoa. Contesta brevemente:

(a) Que permite a opción -v do comando iptables?

(b) Portátil. Executa na anterior consola:

```
# iptables -L -line-numbers -t nat -v
# iptables -Z
# iptables -L -line-numbers -t nat -v
```

Que acontece? Que siginifica a opción -Z do comando iptables?

(c) Por que na práctica empregamos a táboa nat de iptables e non a táboa filter?

(d) Que significan: NAT, SNAT, DNAT, PAT e Port Forwarding? Para que serven? Indica e identifica como mínimo 2 dispositivos de rede que empreguen NAT e/ou SNAT e/ou DNAT e/ou PAT e/ou Port Forwarding.

(e) Indica que fan os seguintes comandos?

I. Comandos:

```
# echo net.ipv4.ip_forward=1 >> /etc/sysctl.conf
# sysctl -p
```

II. Comando:

```
#sysctl -w net.ipv4.ip_forward=1
```

(f) Avisar ao docente para a entrega e revisión da práctica. ☐