TALLER SR – PRÁCTICA 67 – NAT + Bridge + Access Point: berate_ap

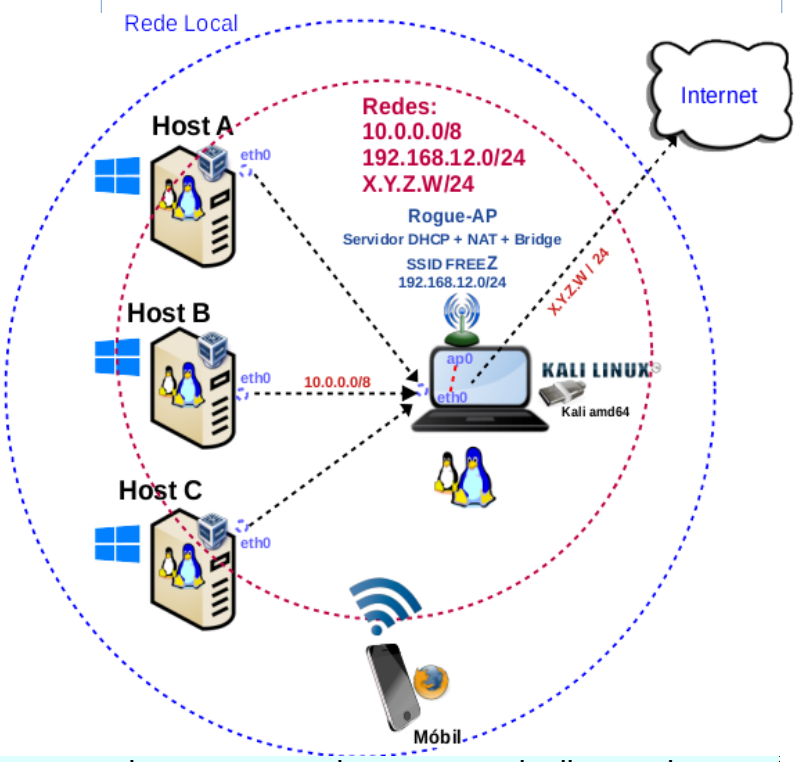
NÚMERO DE GRUPO	FUNCIÓNS	Apelidos, Nome
	Coordinador/a:	
	Responsable Limpeza:	
	Responsable Documentación:	

ESCENARIO: berate-ap (NAT+Bridge+AP)

Portátil:
Rede Local
MAC filtrada (con acceso a Internet)
Rede3: X.Y.Z.W/24 (Internet)
Rede1: 10.0.0.0/8
  IP/MS: 10.10.10.200/8
berate-ap:
  Rede2: 192.168.12.0/24
    IP/MS: 192.168.12.1/24

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
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB
Rede: 10.0.0.0/8
IP/MS: 10.10.10.XY



Material necesario	Práctica: NAT + Bridge + Access Point (berate_ap)
■ Portátil ■ Regleta ■ Switch 5-Port Gigabit ■ USB Live amd64 Kali ■ Hosts alumnado ■ Cableado de rede ■ [1] Práctica 1 ■ [2] Práctica SI Firewall iptables ■ [3] berate-ap ■ [4] Móbiles alumnado ■ [5] Taller SI Práctica 6 ■ [6] Práctica-SI-DNS-DHCP-dnsmasq	(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) Portátil: a) Configurar a rede según escenario. b) Instalar/configurar berate-ap [3] (5) Móbiles alumnado: Acceder con autenticación a Internet mediante os móbiles de alumnado a través do AP (4b) (6) Hosts alumnado: a) Crear máquinas virtuais coa rede en modo “Bridge” e especificacións según escenario. b) Arrancar máquina virtual. Configurar rede según escenario. c) Acceder a Internet. (7) Portátil: Estudar configuración berate-ap [3]: Servidor DHCP, Regras iptables, Enrutamento (bridge)

Procedemento:

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

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

(b) Conectar o switch á regleta.

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

(d) **Conectar o switch á roseta da aula.**

(e) **NON conectar os vosos equipos de alumnado ao switch.**

(2) Portátil:

(a) Arrancar co USB Live Kali amd64.

(b) Comprobar que tedes acceso á rede local e a Internet. Abrir unha consola e executar:

$ setxkbmap es `#Configurar teclado en español`

$ ip addr show eth0 `#Amosar información sobre a NIC eth0. Verificar a configuración de rede para a NIC eth0`

$ 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.`

$ ping -c4 www.google.es `#Enviar 4 paquetes ICMP ECHO_REQUEST a www.google.es, solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede hacia Internet e ao servidor de google.`

(c) Instalar paquete **berate-ap**. Abrir unha consola(consola1) e executar:

$ 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)`

dpkg -l berate-ap ; [$(echo $?) -eq '1'] && apt update && apt -y install berate-ap `#Verificar se o paquete berate-ap está instalado. Se non está instalado, actualízase a lista de paquetes dos repositorios e instálase.`

exit `#Saír da consola.`

$ ip addr show `#Amosar información sobre as NIC. Verificar a configuración de rede para as NIC do sistema`

$ 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.`

$ ping -c4 www.google.es `#Enviar 4 paquetes ICMP ECHO_REQUEST a www.google.es, solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede hacia Internet e ao servidor de google.`

Cubrir a seguinte táboa:

Host Portátil	IP	Máscara Subrede	Gateway	IP Servidores DNS (/etc/resolv.conf)
eth0				
wlan0				
ap0				

(d) Avisar ao docente para a revisión. ☐1

(3) Portátil. Configurar Rogue-AP con autenticación [3] na primeira consola aberta(consola1):

berate_ap -h `#Ver a axuda do comando berate_ap`

Usage: berate_ap [options] <wifi-interface> [<interface-with-internet>] [<access-point-name> [<passphrase>]

...

berate_ap --mana-loud wlan0 eth0 FREE**Z** XXXXXXXXXX `#Xerar un AP con acceso a Internet con contrasinal XXXXXXXXXX a través da NIC wlan0 de nome(SSID) FREEZ (WPA/WPA2 → Contrasinal entre 8 e 63 caracteres). **Substituír Z polo número do grupo**, tal que para o grupo 3: Z=3, sendo o **FREEZ=FREE3** e substituir XXXXXXXXXX polo contrasinal que se considere.`

Cubrir a seguinte táboa:

Host Portátil	IP	Máscara Subrede	Gateway	IP Servidores DNS (/etc/resolv.conf)
eth0				
wlan0				
ap0				

(4) Móbiles alumnado:

(a) Verificar se se visualiza o AP FREE**Z** *(substituír Z polo número do grupo)* .

(b) Verificar se é posible conectar co AP FREE**Z** *(substituír Z polo número do grupo)* con autenticación e indicar o que acontece na consola aberta do portátil (consola1).

Cubrir a seguinte táboa:

Móbil alumnado	MAC Address	Concesión rede ao cliente polo AP (dnsmasq.leases)			
		IP	Máscara Subrede	Gateway	IP Servidores DNS (/etc/resolv.conf)
alumnoXY					
alumnoXY					
alumnoXY					

(c) Verificar se é posible conectar á URL www.github.com/ricardofc e indicar o que acontece na consola aberta do portátil (consola1).

(d) Verificar se é posible autenticar na conta de gmail.com de cada usuario do grupo e indicar o que acontece na consola aberta do portátil (consola1).

(e) Avisar ao docente para revisión. ☐ 2

(5) Portátil. Estudar a configuración berate-ap [3]: Servidor DHCP, Regras iptables, Enrutamento (bridge)

NOTA: Ao xerar no apartado (3) un AP co comando **berate_ap** conseguimos unha saída na consola similar á seguinte:

```
Config dir: /tmp/create_ap.wlan0.conf.eW9Wv8ZL
PID: 14039
Network Manager found, set ap0 as unmanaged device... DONE
Creating a virtual WiFi interface... ap0 created.
Sharing Internet using method: nat
hostapd command-line interface: hostapd_cli -p /tmp/create_ap.wlan0.conf.eW9Wv8ZL/hostapd_ctrl
Configuration file: /tmp/create_ap.wlan0.conf.eW9Wv8ZL/hostapd.conf
Using interface ap0 with hwaddr 42:00:00:00:00:00 and ssid "FREEZ"
ap0: interface state UNINITIALIZED->ENABLED
ap0: AP-ENABLED
```

Entón:

(a) Directorio /tmp/create_ap.wlan0.conf.eW9Wv8ZL *(no voso caso revisar o nome do directorio)* , o cal é o directorio que contén toda a configuración do AP xerado a través do comando **berate_ap**.

ls -l /tmp/create_ap.wlan0.conf.eW9Wv8ZL

total 24

-rw------- 1 root root 235 Feb 19 23:09 **dnsmasq.conf → Ficheiro de configuración do Servidor DHCP**

-rw-r--r-- 1 root root 0 Feb 19 23:09 **dnsmasq.leases → Ficheiro que contén a configuración de rede concedida aos clientes DHCP**

-rw-r--r-- 1 nobody nogroup 6 Feb 19 23:09 dnsmasq.pid

-rw------- 1 root root 304 Feb 19 23:09 **hostapd.conf → Ficheiro de configuración do Rogue-AP xerado**

drwx------ 2 root root 60 Feb 19 23:09 hostapd_ctrl

-rw------- 1 root root 5 Feb 19 23:09 nat_internet_iface

-r--r--r-- 1 root root 6 Feb 19 23:09 pid

-r--r--r-- 1 root root 4 Feb 19 23:09 wifi_iface

(b) Servidor DHCP: dnsmasq

cat /tmp/create_ap.wlan0.conf.*/dnsmasq.conf

listen-address=192.168.12.1 → **IP do AP ($ ip addr show ap0** `#ap0 é a interface virtual do AP xerado`**)**

bind-dynamic

dhcp-range=192.168.12.1,192.168.12.254,255.255.255.0,24h → **Pool de IPs e tempo de concesión**

dhcp-option-force=option:router,192.168.12.1 → **Porta de enlace (gateway) a conceder: 192.168.12.1**

dhcp-option-force=option:dns-server,192.168.12.1 → **Servidor DNS a conceder: 192.168.12.1**

dhcp-option-force=option:mtu,1500

no-hosts → **Non ler os hostnames no ficheiro /etc/hosts**

(c) Regras iptables. Executar os seguinte comandos e **explicar a saída da súa execución (explicar regras)**.

iptables -L `#Listar todas as regras das cadeas da táboa filter, é dicir, amosar todas as regras das cadeas INPUT, FORWARD e OUTPUT.`

Chain INPUT (policy ACCEPT)

target	prot	opt	source	destination	
ACCEPT	udp	--	anywhere	anywhere	udp dpt:bootps
ACCEPT	udp	--	anywhere	anywhere	udp dpt:mdns
ACCEPT	tcp	--	anywhere	anywhere	tcp dpt:5353

Chain FORWARD (policy ACCEPT)

target	prot	opt	source	destination
ACCEPT	all	--	anywhere	192.168.12.0/24
ACCEPT	all	--	192.168.12.0/24	anywhere

Chain OUTPUT (policy ACCEPT)

target	prot	opt	source	destination

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.

Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	
1	0	0	REDIRECT	udp	--	any	any	192.168.12.0/24	192.168.12.1	udp dpt:domain redir ports 5353
2	0	0	REDIRECT	tcp	--	any	any	192.168.12.0/24	192.168.12.1	tcp dpt:domain redir ports 5353

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination
1	0	0	MASQUERADE	all	--	any	!ap0	192.168.12.0/24	anywhere

(d) Enrutamento (bridge). Executar os seguinte comandos e **explicar a saída da súa execución**:

cat /proc/sys/net/ipv4/ip_forward
1
ip route
default via X.Y.Z.1 dev eth0 proto dhcp src X.Y.Z.W metric 100
X.0.0.0/8dev eth0 proto kernel scope link src X.Y.Z.W metric 100
192.168.12.0/24 dev ap0 proto kernel scope link src 192.168.12.1

(6) 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: Practica62-berate-ap-AlumnoXY, *o valor XY é o valor do PC que tedes asignado. Así, o alumno 17 terá como nome da máquina virtual: Practica62-berate-ap-Alumno17*

(b) Arrancar máquina virtual.

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

$ 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

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

(8) Portátil. Configuración na nova rede e comprobar a conectividade de rede coa máquinas virtuais:

ip addr add 10.10.10.10/8 dev eth0 #Configurar a tarxeta de rede eth0, coa IP: 10.10.10.10 e máscara de subrede: 255.0.0.0

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.

(9) Máquinas virtuais dos hosts do alumnado:

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

I. Para a máquina virtual pertencente ao hostA.

ping -c4 10.10.10.10 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostA.

II. Para a máquina virtual pertencente ao hostB.

ping -c4 10.10.10.10 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostA.

III. Para a máquina virtual pertencente ao hostC.

ping -c4 10.10.10.10 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostA.

(b) Comprobar a conectividade de rede cos móbiles do alumnado (ver apartado 4b). Indicar que acontece. Por que?

I. Para a máquina virtual pertencente ao hostA.

ping -c4 IP-Mobil1 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostA.

II. Para a máquina virtual pertencente ao hostB.

ping -c4 IP-Mobil2 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostA.

III. Para a máquina virtual pertencente ao hostC.

ping -c4 IP-Mobil3 #Enviar 4 paquetes ICMP ECHO_REQUEST solicitando 4 paquetes ICMP ECHO_RESPONSE, para verificar a conectividade de rede coa máquina virtual do hostA.

(10) Avisar ao docente para a revisión. ☐3

(11) Razoa. Contesta brevemente:

(a) Portátil. Executa nunha consola:

echo 0 > /proc/sys/net/ipv4/ip_forward

Que acontece se desconectas e conectas de novo o móbil ao SSID configurado (FREE**Z**):

I. O AP segue concedendo configuración de rede aos móbiles do alumnado?

II. Os móbiles do alumnado continúan saíndo a Internet a través do AP?

III. As máquinas virtuais e móbiles de alumnado poden comunicarse en rede (ping)?

(b) Portátil. Executa nunha consola:

echo 1 > /proc/sys/net/ipv4/ip_forward

Que acontece se desconectas e conectas de novo o móbil ao SSID configurado (FREE**Z**):

I. O AP segue concedendo configuración de rede aos móbiles do alumnado?

II. Os móbiles do alumnado continúan saíndo a Internet a través do AP?

III. As máquinas virtuais e móbiles de alumnado poden comunicarse en rede (ping)?

(c) Portátil. Executa nunha consola:

```
# iptables -F -t filter
# iptables -F -t nat
```

Que acontece se desconectas e conectas de novo o móbil ao SSID configurado (FREE**Z**):

I. O AP segue concedendo configuración de rede aos móbiles do alumnado?

II. Os móbiles do alumnado continúan saíndo a Internet a través do AP?

III. As máquinas virtuais e móbiles de alumnado poden comunicarse en rede (ping)?

(d) Avisar ao docente para a entrega e revisión da práctica. ☐ 4

Revisión:

☐ 1 ☐ 2 ☐ 3 ☐ 4