

TALLER SI – PRÁCTICA 6

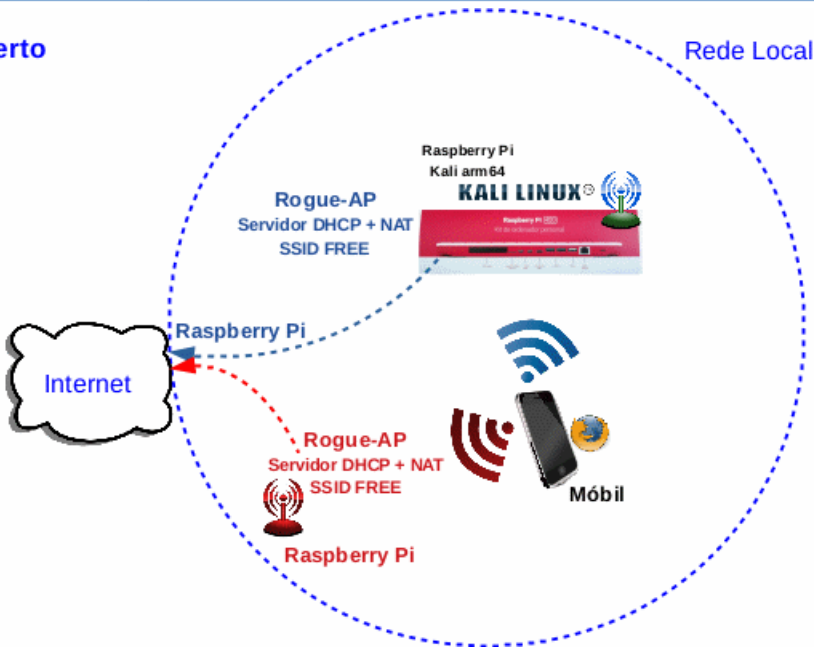
NÚMERO DE GRUPO	FUNCIÓN	Apellidos, Nome
<div></div>	Coordinador/a:	
	Responsable Limpieza:	
	Responsable Documentación:	

ESCENARIO: Rogue AP → SSID FREE → WIFI aberto

Raspberry Pi Grupo:
Servidor DHCP + NAT
Rede Local
Acceso a Internet

Raspberry Pi Taller:
Servidor DHCP + NAT
Rede Local
Acceso a Internet

Móbil alumnado



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

Material necesario	Práctica: Ataque Rogue AP. Desconfiar de AP abertas (sen contrasinal e acceso a Internet)
<ul style="list-style-type: none">■ [1] Práctica 5■ Raspberry Pi 4 (ou 400) con conexión WIFI e acceso a Internet (material que posúe o grupo)■ [2] berate-ap■ Móviles alumnado■ Raspberry Pi 3 (ou 4) con conexión WIFI e acceso a Internet (material existente no taller)■ [3] Firewall iptables	<ul style="list-style-type: none">(1) Prerrequisito: Ter realizada a Práctica 5.(2) Montar Rogue AP na Raspberry Pi (material de grupo)(3) Acceder sen/con autenticación a Internet mediante os móbiles de alumnado a través do Rogue AP configurado no punto (2)(4) Comprobar acceso en 2 AP de idéntico nome(SSID)



Procedemento:

(1) Prerrequisito: Realizar a [Práctica 5](#) [1], co cal a Raspberry Pi ten acceso á rede local e a Internet.

(2) Raspberry Pi 4(ou 400):

(a) Arrancar coa MicroSD (Live amd64 Kali GNU/Linux)

(b) Instalar paquete **berate-ap**: Conseguir acceso á rede local e a Internet. 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.
```

(c) Abrir outra consola(consola2) e executar:

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

```
# [ -f /var/log/syslog ] && tail -f /var/log/syslog || exit #Deixar aberto o ficheiro de rexistro /var/log/syslog para verificar o que acontece no sistema en tempo real se existe o ficheiro /var/log/syslog, no caso contrario saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
```

(d) Abrir unha terceira consola(consola3) e executar:

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

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

```
# iptables --line-numbers -L -t nat #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.
```

(e) Configurar Rogue-AP sen autenticación [2] 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 FREEZ #Xerar un AP con acceso a Internet sen autenticación a través da NIC wlan0 de nome(SSID) FREEZ. Substituír Z polo número do grupo, tal que para o grupo 3: Z=3, sendo o FREEZ=FREE3
```

(3) Móviles alumnado:

(a) Verificar se se visualiza o AP FREEZ (substituír Z polo número do grupo) e indicar o que acontece nas consolas abertas da Raspberry Pi consola1 e consola2. Realiza de novo o apartado 2.d) na consola3. Que acontece? Cal é a saída?

(b) Verificar se é posible conectar co AP FREEZ (substituír Z polo número do grupo) sen autenticación e indicar o que acontece nas consolas abertas da Raspberry Pi consola1 e consola2.

i. Cal é a MAC Address da NIC do móbil? É necesario revisala nos Axustes de configuración do móbil?

ii. Cal é a IP cedida polo Rogue AP? É necesario revisala nos Axustes de configuración do móbil?

iii. Realiza de novo o apartado 2.d) na consola3. Que acontece? Cal é a saída?

iv. Realiza na consola3 os seguintes comandos:

```
# iptables-save > iptables-save.txt #Gardas todas as regras de iptables no ficheiro iptables-save.txt
```

```
# cat iptables-save.txt #Ver o contido do ficheiro iptables-save.txt
```

(c) Verificar se é posible conectar á URL www.github.com/ricardofc e indicar o que acontece nas consolas abertas da Raspberry Pi consola1 e consola2. Na consola3 realiza de novo o apartado 3biv) cambiando o nome do ficheiro a iptables-save-2.txt. Comproba as diferencias mediante o seguinte comando:

```
# diff iptables-save.txt iptables-save-2.txt #Amosar as diferencias entre os 2 arquivos pasados como argumentos ao comando diff
```

(d) Verificar se é posible autenticar na conta de gmail.com de cada usuario do grupo e indicar o que acontece nas consolas abertas da Raspberry Pi consola1 e consola2. Na consola3 realiza de novo o

apartado 3biv) cambiando o nome do ficheiro a iptables-save-3.txt. Comproba as diferencias mediante o seguinte comando:

```
# diff iptables-save-2.txt iptables-save-3.txt #Amosar as diferencias entre os 2 arquivos pasados como argumentos ao comando diff
```

(e) Avisar ao docente para revisión. ☐

(4) Raspberry Pi:

(a) Abortar a execución do Rogue AP premendo (Ctrl+C) na consola da Raspberry Pi onde se ten lanzado o comando `berate_ap`.

(b) Crear de novo un Rogue AP WPA/2 (con autenticación) mediante o seguinte comando:

```
# berate_ap --mana-loud wlan0 eth0 FREEZ 1234567890 #Xerar un AP con acceso a Internet con contrasinal 1234567890 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
```

(c) Realizar de novo os apartados do punto (3) para o novo AP de nome(SSID) FREEZ (substituír Z polo número do grupo). Unha vez rematado avisar de novo ao docente para a revisión. ☐

(5) Raspberry Pi 3 (ou 4) existente no taller(pedir este material ao docente):

NOTA: Z (substituír Z polo número do grupo)

(a) Xerar nesta Raspberri o AP FREEZ (ver punto (3))

(b) Eliminar dos móbiles o AP FREEZ que solicita autenticación (o do punto (4)). Que acontece?

(c) Eliminar dos móbiles os AP FREEZ que tedes gardados no acceso WIFI.

(6) Razoa. Contesta brevemente.

NOTA: Z (substituír Z polo número do grupo)

(a) Agora tedes configurados 2 AP de nome(SSID) FREEZ, un sen autenticación(punto (5)) e outro con autenticación(punto (4)). Intentade acceder cos vosos móbiles:

- Visualizades algún AP FREEZ?
- Conectades a algún deses AP? Se conectades, a cal conectades: o que pide autenticación ou o que non?
- Se podedes conectar aos 2 AP, apagade o AP FREEZ con autenticación (o do punto (4)). Que acontece?

(b) Imos **supoñer** que:

- Na vosa casa tedes un AP de nome(SSID) HOME.
- Tedes gardada a configuración de acceso dese AP no voso móbil.
- Chegades a Aula Taller e mediante a Raspberry Pi configurades un AP sen autenticación de nome(SSID) HOME.

O voso móbil conectariase directamente a ese AP? Solicita algo? Indica algo se non é posible?

(c) Que contramedidas poderíamos tomar para evitar este ataque?

- Deberíamos conectarnos entón a calquera rede WIFI que non solicite autenticación?
- Deberíamos conectarnos entón a calquera rede WIFI que solicite autenticación e non sexa de confianza?
- Deberíamos eliminar sempre a configuración dos AP gardados no móbil? Por que?
- Pode o atacante (cibercriminal) ver en texto claro as comunicacións das conexións dos clientes que acceden a través do Rogue AP? Se non pode, podería chegar a facelo? Que precisaría nese caso?

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