

TALLER SI – PRÁCTICA 7

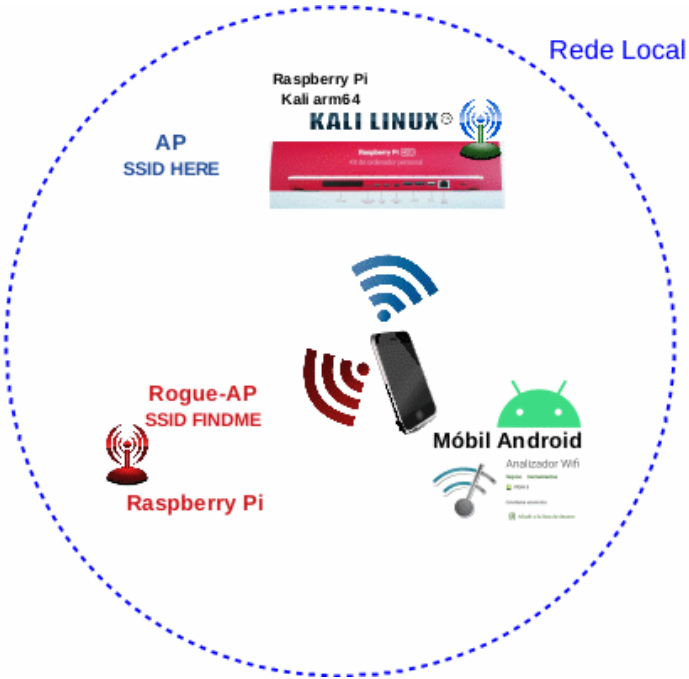
NÚMERO DE GRUPO	FUNCIÓN	Apellidos, Nome
<div></div>	Coordinador/a:	
	Responsable Limpieza:	
	Responsable Documentación:	

ESCENARIO: Rogue AP Oculto

Raspberry Pi Grupo:
Rede Local
AP → SSID: HERE

Raspberry Pi Taller:
Rede Local
Oculto fisicamente
AP → SSID: FINDME

Móbil alumnado Android
Wifi Analyzer farproc



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 6Raspberry Pi 4 (ou 400) con conexión WIFI (material que posúe o grupo)[2] berate-apMóviles alumnado Android[3] Wifi Analyzer farprocRaspberry Pi 3 (ou 4) con conexión WIFI (material existente no taller)[4] Firewall iptables	<ul style="list-style-type: none">(1) Prerrequisito: Ter realizada a Práctica 6.(2) Montar AP na Raspberry Pi (material de grupo)(3) Instalar [3] no móbil do alumnado(4) Consultar app [3] instalada no móbil do alumnado.(5) Atopar o Rogue AP oculto fisicamente (SSID FINDME)



Procedemento:

(1) Prerrequisito: Ter realizada a [Práctica 6](#) [1], co cal xa está instalado o paquete **berate-ap**.

(2) Raspberry Pi 4(ou 400):

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

(b) 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)
# 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 HERE #Xerar un AP con acceso a Internet sen autenticación a través da NIC wlan0 de nome(SSID) HERE
```

(3) Móviles alumnado Android:

(a) Instalar [3]

(b) Abrir a app instalada no paso anterior: Wifi Analyzer.

(c) Facer unha captura da pantalla **Gráfico de canales** e identificar: Cantos AP aparecen? Cales? En que canales? Cal posúe maior intensidade de sinal?

(d) Facer unha captura da pantalla **Lista de AP** e identificar: Cantos AP aparecen? Cales? En que canales? Cal posúe maior intensidade de sinal? Que seguridade e protocolos posúen?

(e) Buscar e definir os protocolos e tecnoloxías WIFI atopadas en cada AP, por exemplo definir:

WPA2, PSK, CCMP, ESS, WPS, K, V

(f) Na pantalla **Medidor de señal** escoller o AP co SSID **FINDME** e:

i. Facer unha captura de pantalla

ii. Activar son

iii. Moverse pola Aula Taller e revisando o medidor da pantalla da app e o son localizar este AP oculto fisicamente. Unha vez atopado este AP avisar ao docente para revisión.

(4) Contesta e razoa brevemente.

(a) Foi fácil atopar o **Rogue AP FINDME**?

(b) Que tal funciona a app Wifi Analyzer?

(c) A app Wifi Analyzer pode servir para determinar cal é a canle WIFI que posúe menos “ruído”, é dicir, server para saber se podemos configurar un AP nunha canle que non esté moi ocupada no espectro electromagnético?

Lineamientos de marca

"El robot de Android se reproduce o modifica a partir del trabajo generado y compartido por Google, y se usa conforme a lo descrito en la Licencia de Atribución de Creative Commons 3.0".