

TALLER SI – PRÁCTICA 8

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

ESCENARIO: Rogue AP → Phishing

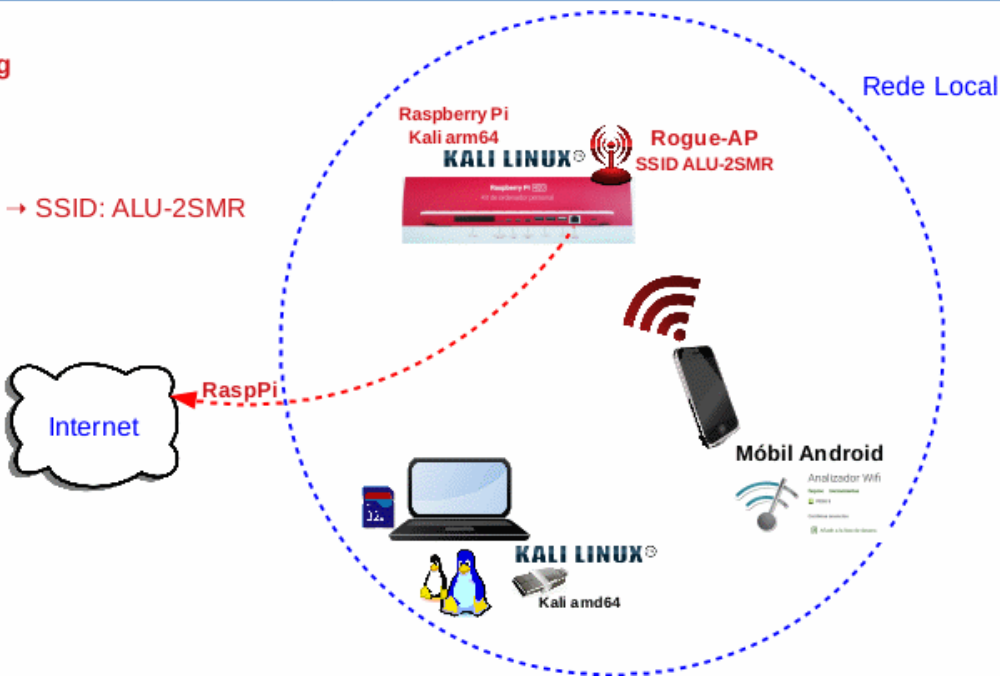
Raspberry Pi Grupo:

Rede Local + Internet

EvilTrust-kali-rpi-Automatic-Boot → AP → SSID: ALU-2SMR

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: Phishing. “Roubo” de credenciais
<ul style="list-style-type: none">■ [1] Práctica 7■ Portátil con acceso a Internet (material existente no taller)■ USB Live amd64 Kali GNU/Linux (solicitar ao docente)■ Raspberry Pi 4 (ou 400) con acceso á rede local e Internet (material que posúe o grupo)■ [2] Descargas Kali ARM■ [3] Documentación Kali ARM■ [4] Repositorio evilTrust-kali-rpi-Automatic-Boot■ [5] README.md■ Móviles alumnado Android■ [6] Wifi Analyzer farproc■ [7] Práctica SI Firewall iptables	<ul style="list-style-type: none">(1) Prerrequisito: Ter realizada a Práctica 7.(2) Portátil:<ul style="list-style-type: none">a) Descargar a distribución Kali ARM (arm64) e verificar a súa descarga.b) Conectar a tarxeta MicroSD co adaptador SD no portátilc) Crear MicroSD arrancable(3) Raspberry PI<ul style="list-style-type: none">a) Arrancar mediante a MicroSD Kalib) Cambiar contrasinais de usuariosc) Clonar repositorio [3]d) Acceder dentro do repositorio e executar script <i>automatic-kali-rpi.sh</i>e) Rogue AP lanzado a espera de “víctimas”



Procedemento:

(1) Portátil:

- (a) Arrancar cun USB Live amd64 Kali GNU/Linux
- (b) Descargar [Kali arm64](#) [2] en /home/kali
- (c) Verificar descarga mediante comprobación hash. Exemplo:

```
$ pwd #Imprimir directorio de traballo actual
/home/kali
$ sha256sum kali-linux-2021.4-rpi-arm64.img.xz #Calcular Hash sha256
```

(d) Conectar a tarxeta MicroSD mediante o adaptador SD no portátil

\$ sudo dmesg -w #Antes de conectar executar este comando. A continuación da execución conectar. Pódese verificar o nome do dispositivo conectado, por exemplo: mmcblk0

(e) [Crear a MicroSD arrancable](#)[3]. Exemplo:

```
$ mount #Importante!: Verificar que o dispositivo non está montado
$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando
sudo (/etc/sudoers, visudo)
# xzcat /home/kali/kali-linux-2021.4-rpi-arm64.img.xz | dd of=/dev/mmcblk0 bs=4M \
status=progress #"Queimar" microSD
# exit #Saír da shell
$ mount #Importante!: Verificar que o dispositivo non está montado. Se non está montado sacar a
tarxeta MicroSD(adaptador SD) do portátil
```

(2) Raspberry Pi:

- (a) Conectar a MicroSD na Raspberry Pi
- (b) Arrancar e verificar o arranque do sistema operativo Kali ARM (arm64)
- (c) Modificar contrasinais de usuarios kali e root. Novos contrasinais **abc123**. (Ollo que existe un caracter punto e final no contrasinal!). Exemplo:

```
$ echo -e 'kali\nabc123.\nabc123.' | passwd #Cambiar contrasinal ao usuario kali
$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando
sudo (/etc/sudoers, visudo)
# echo -e 'abc123.\nabc123.' | passwd #Cambiar contrasinal ao usuario root
```

(d) Clonar o repositorio [4]:

```
# git clone https://github.com/ricardofc/evilTrust-kali-rpi-Automatic-Boot.git
```

(e) Avisar ao docente para revisión.

(3) Móviles alumnado Android:

- (a) Instalar [6]
- (b) Abrir a app instalada no paso anterior: Wifi Analyzer.
- (c) Facer unha captura da pantalla **Gráfico de canales**
- (d) Facer unha captura da pantalla **Lista de AP**
- (e) Pechar a app Wifi Analyzer.

(4) Executar[5]:

```
# cd evilTrust-kali-rpi-Automatic-Boot #Acceder ao contido do repositorio
# bash automatic-kali-rpi.sh #Executar o script automatic-kali-rpi.sh que permitirá tras a súa
execución que a Raspberry Pi a partir do próximo reinicio arranque automaticamente na contorna gráfica
co usuario root(sen solicitar contrasinal) e sexa executada esta ferramenta lanzándose o Rogue AP á
espera de "víctimas"
```

(5) Avisar ao docente para revisión.

- (6) Realizar de novo os apartados 3.b, 3.c e 3d. Contesta e razoa brevemente.
- (a) Atopades o **Rogue AP ALU-2SMR**? Cantos **ALU-2SMR** aparecen? Por que?
 - (b) Compara a MAC Address da NIC wlan0 da Raspberry PI e o bssid de todos os **Rogue AP ALU-2SMR**. Hai algunha que coincide? Por que?
 - (c) Amosa a saída da execución dos seguintes comandos [7]:

```
# iptables -L
# iptables -L -t nat
# cat /proc/sys/net/ipv4/ip_forward
```

Que indica esa saída?

- (7) Móbil alumnado: Conectar ao **Rogue AP ALU-2SMR**
- (a) Que acontece? Captura as pantallas do procedemento de conexión.
 - (b) Introduce unhas credenciais ficticias e valídate na páxina. Que acontece?
 - i. Captura unha imaxe da pantalla da Raspberry Pi.
 - ii. Accede ao cartafol *ies-ald-login* e amosa o contido do ficheiro *datos-privados.txt*
 - (c) Abre unha nova páxina e accede a www.google.es. Intenta conectarte a outras páxinas web? Que acontece?
 - (d) Aborta[5] a execución do **Rogue AP ALU-2SMR** premendo **Ctrl+C**. Que acontece?
 - i. Captura unha imaxe da pantalla da Raspberry Pi.
 - ii. Accede ao cartafol *ies-ald-login* e amosa o contido do ficheiro *datos-privados*.txt*
 - iii. Realiza de novo os apartados 3.b, 3.c e 3d.
 - iv. Realiza de novo o apartado 6c.

- (8) Executar[5]:
- ```
bash utilities/change-cmdline.sh TP_LINK 11 #Modificar o SSID e o channel do "ataque"
para ter en conta na próxima execución da ferramenta (reboot → /root/.bashrc → exec.sh → evilTrust.sh → /proc/cmdline).
reboot
```

- (9) Realizar de novo os apartados (6) e (7) pero tendo en conta que o **SSID** xa non é **ALU-2SMR** senón **TP\_LINK**