

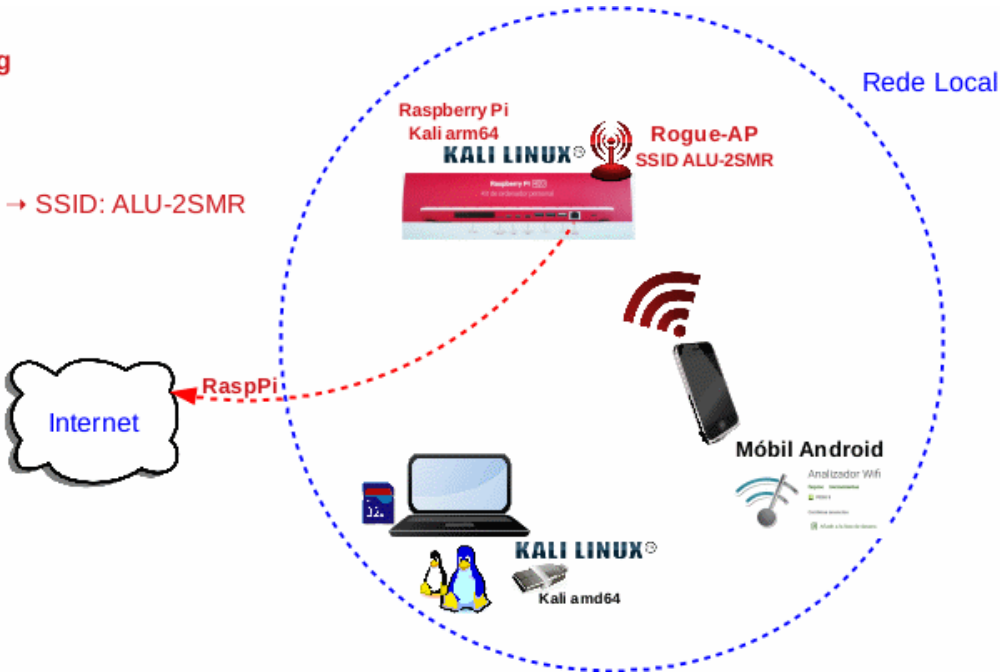
TALLER SI – PRÁCTICA 9

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 Portal Cautivo
<ul style="list-style-type: none">■ [1] Práctica 8■ Raspberry Pi 4 (ou 400) con acceso á rede local e Internet (material que posúe o grupo)■ [2] Repositorio evilTrust-kali-rpi-Automatic-Boot■ [3] README.md■ Móviles alumnado Android■ [4] Wifi Analyzer farproc■ [5] Práctica SI Firewall iptables■ [6] Práctica SI DNS DHCP dnsmasq	<ul style="list-style-type: none">(1) Prerrequisito: Ter realizada a Práctica 8 [1](2) Raspberry PI<ul style="list-style-type: none">a) Rogue AP lanzado a espera de “víctimas”b) Modificar SSID, channel do Rogue AP mediante <i>utilities/change-cmdline.sh</i>c) Reiniciard) Comprobar configuración <i>iptables</i> e <i>dnsmasq</i>e) Acceder a diversos sitios webf) Modificar <i>/etc/hosts</i> e acceder a diversos sitios webg) Modificar directiva <i>address</i> en <i>dnsmasq.conf</i> (<i>eviltTrust.sh</i>)h) Reiniciari) Acceder de novo aos anteriores sitios web (apartado e) (apartado f) → Portal Cautivo



Procedemento:

(1) Realizar a Práctica 8, tal que agora teremos lanzado un **Rogue AP TP_LINK** na canle **11**

(2) Raspberry Pi.

NOTA: N=número de grupo, SSID=GrupoN, channel=N. Por exemplo, se:
Número de grupo=5 → SSID=Grupo5, channel=5

(a) [3] Abrir outro terminal e executar:

```
# bash utilities/change-cmdline.sh Grupo5 5 #cambiar 5 polo número de grupo correspondente. 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
```

(b) [5][6] Unha vez reiniciado e en execución o **Rogue AP** abrir outro terminal e executar:

```
# iptables -L -line-numbers #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 -L -line-numbers -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.  
# grep dnsmasq.conf evilTrust.sh #Buscar o patrón dnsmasq.conf no ficheiro evilTrust.sh  
# cat /root/evilTrust-kali-rpi-Automatic-Boot/dnsmasq.conf #Ver o contido do ficheiro de configuración dnsmasq.conf
```

(c) Capturar as saídas dos comandos anteriores (apartado 2b).

(3) Móviles alumnado Android:

(a) Instalar [4]

(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.

(f) Conectar ao **Rogue AP GrupoN**, onde N=número de grupo.

(g) Abre unha nova páxina e accede a www.google.es. Intenta conectarte a outras páxinas web? Que acontece? Por que?

(4) Raspberry Pi

(a) Executar:

```
# echo '172.16.31.1 6w.edu.xunta.es 6w.edu.xunta.gal' >> /etc/hosts #Engadir en /etc/hosts unha liña: a resolución DNS local 6w.edu.xunta.es e 6w.edu.xunta.gal para que se resolvan na IP 172.16.31.1 pertencente á NIC wlan0  
# echo '172.16.31.1 www.google.es' >> /etc/hosts #Engadir en /etc/hosts unha liña: a resolución DNS local www.google.es para que se resolva na IP 172.16.31.1 pertencente á NIC wlan0  
# cat /etc/hosts #Ver o contido do ficheiro /etc/hosts
```

(b) Capturar as saídas dos comandos anteriores (apartado 4a).

(5) Móviles alumnado Android:

(a) Conectar ao **Rogue AP GrupoN**, onde N=número de grupo.

(b) Abre unha nova páxina e accede a: 6w.edu.xunta.es, 6w.edu.xunta.gal, www.google.es. Intenta conectarte a outras páxinas web? Que acontece? Por que?

(6) Executar:

```
# LINE=$(grep -n dnsmasq.conf evilTrust.sh | grep -v '##' | grep connectivity)
# NUMBER=$(echo $LINE | cut -d':' -f1)

# sed -i "${NUMBER}s/^/#COMENTARIO/g" evilTrust.sh #Con estes 3 últimos comandos comentamos
a directiva address de dnsmasq.conf en evilTrust.sh


# LINE=$(grep -n dnsmasq.conf evilTrust.sh | grep '#/172')
# NUMBER=$(echo $LINE | cut -d':' -f1)

# sed -i "${NUMBER}s/####/ /g" evilTrust.sh #Con estes 3 últimos comandos
descomentamos(activamos) a directiva address de dnsmasq.conf en evilTrust.sh


# reboot
```

(7) Realizar de novo todos os apartados dos exercicios 2, 3 e 5 agás os apartado (2a) e (3a)

(8) Avisar ao docente para revisión.