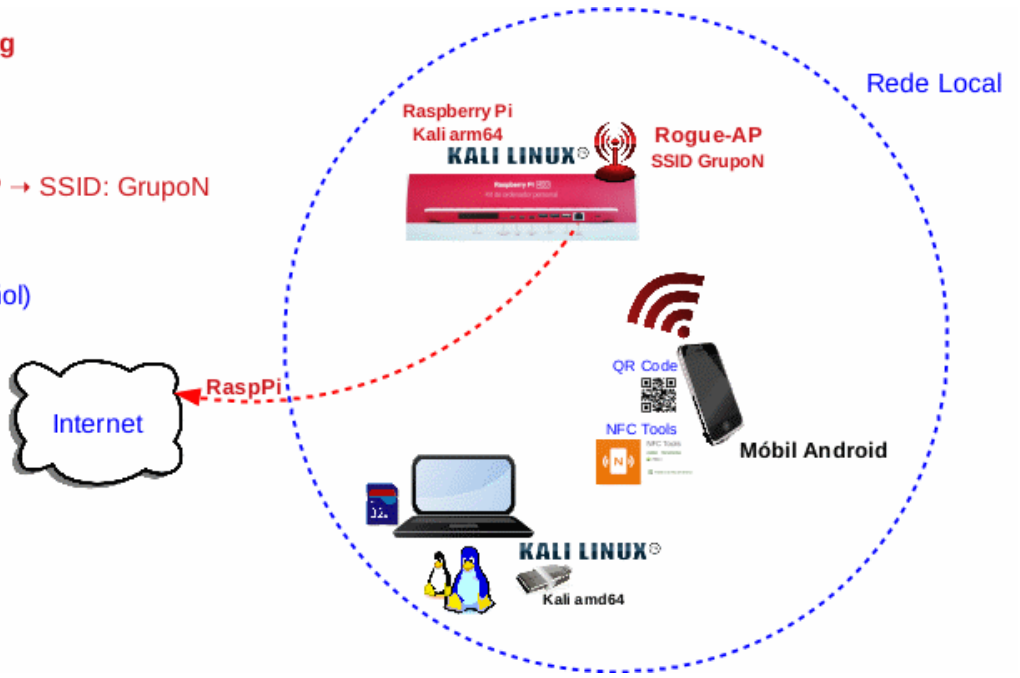
TALLER SI – PRÁCTICA 10		
NÚMERO DE GRUPO	**FUNCIÓNS**	**Apelidos, Nome**
	Coordinador/a:	
	Responsable Limpeza:	
	Responsable Documentación:	

ESCENARIO: Rogue AP → Phishing

Raspberry Pi Grupo:
Rede Local + Internet
EvilTrust-kali-rpi-Automatic-Boot → AP → SSID: GrupoN

Móbil alumnado Android
Lector de códigos QR y barras (español)
NFC Tools



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 QR Code / NFC Stickers
■ [1] Práctica 9 ■ 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 ■ Móbiles alumnado Android ■ NFC Stickers(solicitar ao docente) ■ [4] Lector de códigos QR y barras (español) ■ [5] NFC Tools	(1) Prerrequisito: Ter realizada a Práctica 9 [1] (2) Raspberry PI a) Rogue AP lanzado a espera de "*víctimas*" (3) Móbiles alumnado a) Escanear códigos QR b) Escanear NFC Stickers (4) Raspberri PI a) Descomentar entrada para resolución DNS local (*evilTrust.sh → dnsmasq.conf → /etc/hosts*) (5) Repetir apartado (3)

Procedemento:

(1) Realizar a Práctica 9 [1], tal que agora teremos lanzado un **Rogue AP GrupoN** na canle **5**

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

(2) Móbiles alumnado Android:

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

(b) Instalar [4]

i. Abrir a app instalada no paso anterior: Lector de códigos QR y barras (español).

ii. Escanear os seguintes códigos QR e indicar que acontece:

Acceso Aula Virtual	
Figura 1: QR Code	*Figura 2: QR Code*

iii. Pechar a app [4]

(c) Instalar [5]

i. Abrir a app instalada no paso anterior: NFC Tools

ii. Ler as 2 etiquetas NFC (pegatinas NFC solicitadas ao docente) e indicar que acontece.

iii. Pechar a app [5]

(3) Raspberry PI. Abrir outro terminal e executar:

```
# LINE=$(grep -n 3w.edu.xunta.gal evilTrust.sh)
# NUMBER=$(echo $LINE | cut -d':' -f1)
# sed -i "${NUMBER}s/##//g" evilTrust.sh #Con estes 3 últimos comandos descomentamos(activamos) a resolución DNS local de 3w.edu.xunta.gal a través de dnsmasq
# reboot
```

(4) Realizar de novos os apartados 2bi, 2bii, 2biii e 3ci, 3cii e 3ciii

(5) Contesta e razoa brevemente:

(a) Podemos confiar nos códigos QR a escanear?

(b) Podemos confiar nos stickers NFC a escanear?

(c) Nesta práctica, que tecnoloxía parécevos máis útil? Por que?