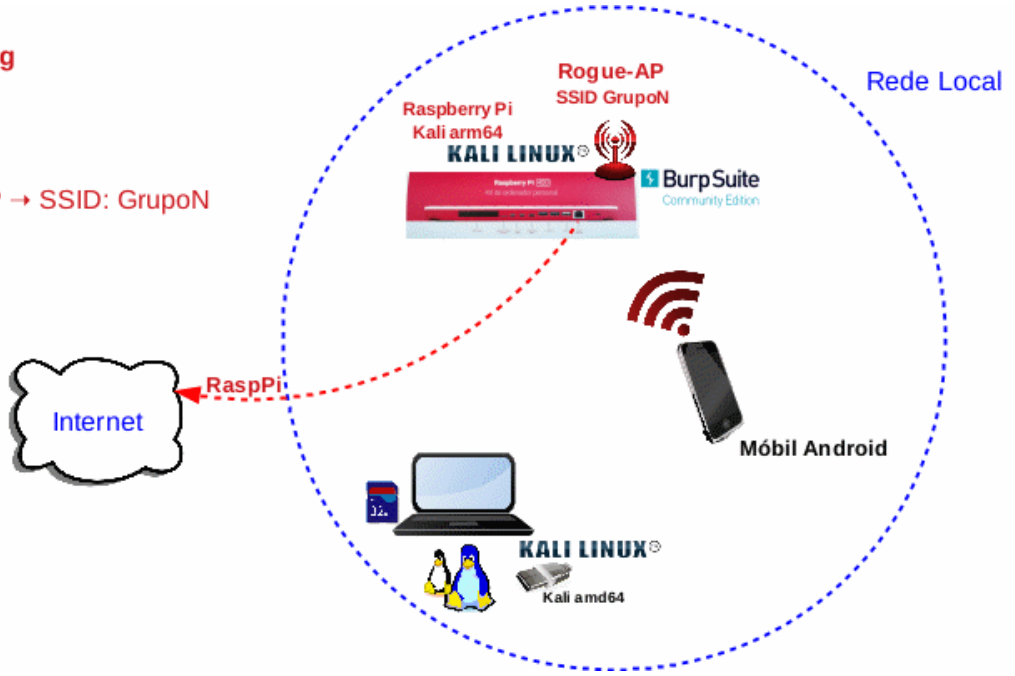
TALLER SI – PRÁCTICA 12		
NÚMERO DE GRUPO	**FUNCIÓNS**	**Apelidos, Nome**
	Coordinador/a:	
	Responsable Limpeza:	
	Responsable Documentación:	

ESCENARIO: Rogue AP → Phishing

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

Móbil alumnado Android



Material necesario	Práctica: Phishing. “Roubo” de credenciais Proxy
■ [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 ■ [4] burpsuite ■ [5] Burpsuite CA Certificate Android ■ [6] Installing BURP Digital Security Certificate on Android .DER File ■ [7] Añadir y quitar certificados	(1) Prerrequisito: Ter realizada a Práctica 9 [1] (2) Raspberry PI a) Rogue AP lanzado a espera de “*víctimas*” (3) Proxy: burpsuite a) Interceptar comunicacións. b) Alterar comunicacións.

Procedemento:

(1) Realizar a Práctica 9 [1], tal que agora teremos lanzado un **Rogue AP GrupoN** na canle **5.** A este terminal ímolo denominar **terminalA**.

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

(2) Raspberry Pi: **Proxy Burp Suite Community Edition**[4]

Ata agora estivimos interceptando as comunicacións, mediante esta ferramenta ademais podemos modificar/interactuar coas comunicacións.

(a) Antes da conexión de calquera víctima imos sniffar o tráfico POST para ver que como as comunicacións teñen lugar mediante o protocolo HTTP (sen cifrado) e polo tanto tamén se poden visualizar as credenciais unha vez introducidas. Para iso, executar nun novo terminal(identificado como ***terminalB***) :

```
# command -v burpsuite ; [ $? -ne 0 ] && apt update && apt -y install burpsuite #Instalar o paquete burpsuite no caso de non estar instalado
# burpsuite & #Lanzar o Proxy Burp Suite
```

(b) Aceptar todas diálogos de texto que aparezan (Premer **OK** → **I Accept** → **Next** → **Start Burp**)

(c) Desactivar **Intercept** premendo en **Menú** → **Proxy** → **Intercept is on**. Agora o estado é **Intercept is off**.

(d) **Menú** → **Proxy** → **Options** → **Proxy Listeners**

i. Seleccionar **127.0.0.1:8080** e premer en **Remove** → **Yes**

ii. Premer en **Add** → **Bind to port: 8080** → **Especific address:** *Escoller a IP 172.16.31.1* → **OK**

(e) Activar **Intercept** premendo en **Menú** → **Proxy** → **Intercept is off**. Agora o estado é **Intercept is on**.

(f) Avisar ao docente para revisión. ☐$_1$

(3) Móbiles alumnado Android:

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

(b) Axustes WIFI → Manter seleccionado conexión **Rogue AP GrupoN** → Modificar rede → Mostrar opcións avanzadas → Proxy → Manual:

Nome de host de proxy: **172.16.31.1**

Porto proxy: **8080**

Gardar

(c) Podes introducir unhas credenciais ficticias e validarte na páxina. Que acontece?

(d) Avisar ao docente para revisión. ☐$_2$

(4) Raspberry Pi:

(a) Captura unha imaxe do **terminalA**.

(b) Captura unha imaxe do contido da sección Intercept (**Menú** → **Proxy** → **Intercept**).

(c) Premer en **Drop**

(d) Realizar de novo os apartados (3a) e (3c) pero agora na sección **Intercept** premer en **Forward** as veces que sexan necesarias ata que apareza a páxina web (FAKE-Phising) no móbil:

i. Captura unha imaxe do contido da sección HTTP History do Burp Suite(**Menú** → **Proxy** → **HTTP history**).

ii. Captura unha imaxe da pantalla principal do Burp Suite Community Edition (**Menú** → **Dashboard**).

iii. Desactiva **Intercept** premendo en **Menú** → **Proxy** → **Intercept is on**. Agora debe aparecer **Intercept is off**.

iv. Limpa o historial (**Menú** → **Proxy** → **HTTP History** → **Clic botón dereito en calquera páxina do historial** → **Clear history** → **Yes**)

v. Captura unha imaxe do **terminalA**.

(e) Abre unha nova páxina e accede a 172.16.31.1 Podes introducir unhas credenciais ficticias e validarte na páxina. Que acontece?

i. Captura unha imaxe do contido da sección HTTP History do Burp Suite (**Menú → Proxy → HTTP history)**.

ii. Selecciona en **HTTP history** a entrada **POST /post.php** Que acontece? Captura unha imaxe.

iii. Limpa o historial (**Menú → Proxy → HTTP History → Clic botón dereito en calquera páxina do historial → Clear history → Yes**)

(f) Abre unha nova páxina e accede a www.gmail.com Podes introducir unhas credenciais ficticias e validarte na páxina. Que acontece?

i. Captura unha imaxe do contido da sección HTTP History do Burp Suite (**Menú → Proxy → HTTP history)**.

ii. **Móbil**. Captura unha imaxe do móbil

(g) Realiza o procedemento descrito en [5][6][7] para instalar o certificado CA Burp Suite en VPN/Aplicacións. Basicamente:

i. Descargar certificado:

Abrir ***http://172.16.31.1:8080*** → Premer en ***CA Certificate*** → Gardar coa extension cer (**cacert.cer**)

ii. Instalar certificado:

Axustes → Buscar a cadea *credenciales* → **Cifrado y credenciales → Credenciales de usuario → Instalar desde almacenamiento → Buscar e Seleccionar CA Burp Suite (cacert.cer) → Instalar → VPN y aplicaciones → Instalar**

(h) Realiza de novo o apartado (4f).

(i) Avisar ao docente para revisión. ☐$_3$

(j) Desactiva o proxy da configuración do móbil(ver apartado 3b)

(k) Desinstala do móbil o certificado do apartado (4g) (Axustes → Buscar a cadea *credenciales* → **Cifrado y credenciales → Credenciales de usuario → Seleccionar CA Burp Suite → Eliminar**)

(5) Móbiles alumnado Android:

(a) Desconectase do **Rogue AP GrupoN**

(b) Conectarse de novo ao **Rogue AP GrupoN**

(6) Raspberry Pi: Sección Intercept → Alterar comunicacións

(a) ***(Estado Intercept is off)*** Abre unha nova páxina e accede a 172.16.31.1

(b) Activa **Intercept** premendo en **Menú → Proxy → Intercept is on**. Agora debe aparecer **Intercept is on**.

(c) Introducir as seguintes credenciais ficticias e intenta validarte na páxina:

usuario → **GrupoN** *(onde N é o número do grupo)*

contrasinal → **abc123.**

(d) Se é necesario premer en **Forward** ata que apareza no burpsuite a petición **POST /post.php** referente á páxina web (FAKE-Phishing Aula Virtual).

(e) Debes estar a ver unha entrada similar á seguinte:

```
email_aulaVirtual=Grupo5&password_aulaVirtual=abc123.&hostname=XXXXXXXXXXXX&mac=11%
22%33%44%55%66&ip=172.16.31.1&target=http%3A%2F%2Fwww.edu.xunta.gal%2Fcentros
%2Fieslosadadieguez%2Faulavirtual%2Flogin%2Findex.php
```

Captura unha imaxe deste pantalla do burpsuite.

(f) Modificar no proxy burpsuite os valores de *usuario* e *contrasinal*. Para iso, seleccionar eses valores e sobrescribilos polos seguintes:

```
email_aulaVirtual=FAKE&password_aulaVirtual=PHISHING&hostname=XXXXXXXXXXXX&mac=11%
22%33%44%55%66&ip=172.16.31.1&target=http%3A%2F%2Fwww.edu.xunta.gal%2Fcentros
%2Fieslosadadieguez%2Faualvirtual%2Flogin%2Findex.php
```

Captura unha imaxe deste pantalla do burpsuite.

(g) Avisar ao docente para revisión. ☐4

(h) Unha vez modificadas as credenciais premer en **Forward** ata que sexan validadas. Que acontece?

(i) Captura unha imaxe do **terminalA**.

(j) Captura unha imaxe do contido da sección HTTP History do Burp Suite (**Menú → Proxy → HTTP history)**.

(k) Selecciona en **HTTP history** a **última entrada POST /post.php** referente a **http://172.16.31.1**

i. Captura unha imaxe que amose a sección **Original request**

ii. Captura unha imaxe que amose a sección **Edited request**

(l) Limpa o historial (**Menú → Proxy → HTTP History → Clic botón dereito en calquera páxina do historial → Clear history → Yes**)

(m) Avisar ao docente para a entrega e revisión da práctica. ☐5

Revisión:

☐1 ☐2 ☐3 ☐4 ☐5