

# Índice

<b>Prólogo .....</b>	<b>17</b>
----------------------	-----------

## Capítulo I

<b>Inicio con Raspberry Pi .....</b>	<b>19</b>
--------------------------------------	-----------

<b>1. ¿Qué es Raspberry Pi? .....</b>	<b>19</b>
---------------------------------------	-----------

<b>2. Familia Raspberry Pi .....</b>	<b>19</b>
--------------------------------------	-----------

Modelo Raspberry Pi 1 .....	20
-----------------------------	----

Modelo Raspberry Pi 2 .....	20
-----------------------------	----

Modelo Raspberry Pi 3 .....	21
-----------------------------	----

Modelo Raspberry Pi 4 .....	22
-----------------------------	----

<b>3. Familia Raspberry Pi Zero .....</b>	<b>24</b>
---	-----------

Raspberry Pi Zero .....	24
-------------------------	----

Raspberry Pi Zero W .....	25
---------------------------	----

Comparativa modelos de Raspberry Pi .....	25
---	----

<b>4. Raspbian .....</b>	<b>26</b>
--------------------------	-----------

Instalar Raspbian con Etcher .....	27
------------------------------------	----

<b>5. Instalar Raspbian con Noobs .....</b>	<b>29</b>
---	-----------

Instalar Noobs .....	30
----------------------	----

Instalación de un sistema operativo con Noobs .....	32
---	----

<b>6. Acceso a la Raspberry Pi .....</b>	<b>34</b>
--	-----------

Localización de la Raspberry Pi en el segmento de red .....	35
---	----

Configuración de un cliente WiFi en Raspbian .....	37
--	----

## Capítulo II

<b>Configuración inicial de Raspbian en Raspberry Pi con raspi-config ..</b>	<b>39</b>
--	-----------

<b>1. Comenzando con raspi-config .....</b>	<b>39</b>
---	-----------

<b>2. Opciones de configuración desde raspi-conf .....</b>	<b>40</b>
--	-----------

Change User Password .....	40
----------------------------	----

Network Options .....	41
-----------------------	----

**Capítulo III**

<b>Raspberry Pi, USB Canary y el Bot de Telegram .....</b>	<b>61</b>
<b>1. Introducción.....</b>	<b>61</b>
<b>2. Unidades USB en Raspbian.....</b>	<b>61</b>
USBmount.....	62
<b>3. Creación de un bot en Telegram .....</b>	<b>64</b>
Obtención del token del bot .....	65
<b>4. Instalación de telepot.....</b>	<b>66</b>
Prueba de la cuenta.....	66
Recibir mensajes .....	67
Enviar un mensaje.....	68
<b>5. USB Canary .....</b>	<b>68</b>
Descarga de USB Canary.....	68
Dependencias necesarias.....	69
Fichero settings.json.....	70
<b>6. Detectar la conexión y desconexión de un pendrive en los puertos USB.....</b>	<b>72</b>

**Capítulo IV**

<b>GPIO .....</b>	<b>73</b>
<b>1. Introducción.....</b>	<b>73</b>
<b>2. ¿Qué son las GPIO? .....</b>	<b>73</b>
<b>3. Conexión de dispositivos.....</b>	<b>76</b>
<b>4. Lenguajes de programación .....</b>	<b>80</b>
Hola mundo.....	83
Entradas GPIO .....	84
<b>5. SPI - Nuestra Raspberry como clonador de tarjetas .....</b>	<b>86</b>

**Capítulo V**

<b>FruityWifi Raspberry Pi.....</b>	<b>95</b>
<b>1. Instalación de FruityWiFi en Raspberry Pi.....</b>	<b>95</b>
<b>2. Instalación de módulos.....</b>	<b>99</b>
<b>3. Interfaz de red en Modo Hostapd .....</b>	<b>100</b>
Creación de un punto de acceso.....	101
<b>4. URLSnarf.....</b>	<b>103</b>
<b>5. DNSspooF.....</b>	<b>104</b>

<b>6. Ngrep .....</b>	<b>105</b>
<b>7. SSLstrip.....</b>	<b>107</b>
<b>8. Interfaz de red en Modo Monitor .....</b>	<b>108</b>
Mdk3 .....	109
<b>9. WiFiRecon.....</b>	<b>111</b>
<b>10. Karma.....</b>	<b>112</b>

## Capítulo VI

### Denegación de Servicio en Redes WiFi con Raspberry Pi ..... 115

<b>1. Instalación de MDK4 .....</b>	<b>117</b>
<b>2. Características de MDK4 .....</b>	<b>119</b>
<b>3. Uso de MDK4.....</b>	<b>120</b>
PoC: uso de MDK4 con una interfaz de red .....	120
PoC: uso de MDK4 con dos interfaces de red .....	121
<b>4. Problemas con MDK4 .....</b>	<b>122</b>
<b>5. Modos de ataque en MDK4 .....</b>	<b>124</b>
ATTACK MODE b: Beacon Flooding .....	124
PoC: Attack Mode b .....	125
ATTACK MODE a: Authentication Denial-Of-Service.....	126
PoC: Attack Mode a .....	126
ATTACK MODE p: SSID Probing and Bruteforcing .....	127
ATTACK MODE d: Deauthentication and Disassociation .....	127
PoC: Attack Mode d .....	128
ATTACK MODE m: Michael Countermeasures Exploitation.....	130
ATTACK MODE e: EAPOL Start and Logoff Packet Injection.....	131
ATTACK MODE f: Packet Fuzzer .....	131
<b>6. Referencias .....</b>	<b>132</b>

## Capítulo VII

### Analizador de Red..... 133

<b>1. Introducción.....</b>	<b>133</b>
<b>2. Escaneo de redes y hosts .....</b>	<b>133</b>
Iwlist.....	133
NMAP .....	135
Netdiscover .....	138
Nbtscan.....	139
Tcpdump.....	140

Wireshark .....	141
Metasploit.....	145
<b>3. Creando nuestro propio analizador en Raspberry.....</b>	<b>147</b>
<b>4. Conclusiones .....</b>	<b>153</b>

## Capítulo VIII

<b>Raspberry como nodo TOR .....</b>	<b>155</b>
1. Servicio anónimo en la red TOR.....	160
2. Dominios .onion .....	161
3. Consideraciones sobre la red TOR .....	163

## Capítulo IX

<b>MQTT con Mosquitto.....</b>	<b>165</b>
1. Introducción.....	165
2. Esquema de red .....	166
3. Configuración Básica .....	167
Broker.....	167
Subscriber .....	168
Publicador .....	170
4. Configuración con seguridad básica.....	171
Broker.....	171
Suscriptor .....	174
Publicador .....	175
5. Uso de TLS para cifrar el tráfico. ....	176
Creación de certificados .....	176
Firmamos la clave del bróker .....	179
Broker.....	180
Suscriptor .....	182
Publicador .....	183
Permisos por topic.....	184
Bróker.....	184

## Capítulo X

<b>USB Over IP .....</b>	<b>187</b>
1. Que es USB Over IP .....	187
2. Esquema de red .....	187

<b>3. Instalación .....</b>	<b>188</b>
Instalación y configuración del servidor .....	188
Instalación y configuración del cliente .....	190

## Capítulo XI

<b>PoisonTad.....</b>	<b>195</b>
<b>1. Introducción.....</b>	<b>195</b>
<b>2. ¿Por qué Raspberry Pi Zero?.....</b>	<b>195</b>
<b>3. Ataque mediante PoisonTap .....</b>	<b>196</b>
Estructura y funcionamiento .....	196
Instalación de los componentes.....	197
<b>4. Instalación del Servidor PoisonTap .....</b>	<b>202</b>
<b>5. Probando PosionTap .....</b>	<b>207</b>
Consideraciones a tener en cuenta .....	209
<b>6. Mitigación del ataque.....</b>	<b>210</b>

## Capítulo XII

<b>Open VPN .....</b>	<b>211</b>
<b>1. Qué es una VPN.....</b>	<b>211</b>
<b>2. Esquema de red .....</b>	<b>212</b>
<b>3. Instalación y configuración del servidor .....</b>	<b>213</b>
Instalación de programas necesarios .....	213
Creación de una CA .....	213
Creación de los certificados del servidor .....	216
Creación de los certificados del cliente.....	218
Creación de las claves DH y tls-auth .....	220
Configuración del servidor OpenVPN .....	221
<b>4. Revocar certificados de cliente .....</b>	<b>224</b>
<b>5. Instalación y configuración del cliente .....</b>	<b>225</b>
Instalación de programas necesarios .....	226

## Capítulo XIII

<b>OpenWRT.....</b>	<b>229</b>
<b>1. Qué es OpenWrt .....</b>	<b>229</b>
<b>2. Instalación de OpenWrt.....</b>	<b>229</b>
<b>3. Primera conexión.....</b>	<b>231</b>

<b>4. Configuración Básica .....</b>	<b>234</b>
Creación de contraseña para root .....	235
Configuración de red wifi (Punto de acceso) .....	236
Fecha y Hora .....	241
<b>5. Configuración Avanzada .....</b>	<b>242</b>
Esquema de red deseado .....	243
Configuración .....	243
Port Forwarding .....	250
Asignación estática de dirección IP por MAC .....	252
<b>6. Bloqueador de publicidad.....</b>	<b>254</b>

## Capítulo XIV

<b>AP + SSH + TOR.....</b>	<b>259</b>
<b>1. Qué es un punto de acceso (AP) .....</b>	<b>259</b>
<b>2. Esquema de red .....</b>	<b>260</b>
<b>3. Instalación del AP .....</b>	<b>260</b>
Configuración del servidor dhcp .....	262
Configuración del punto de acceso .....	264
<b>4. Instalación de SSH .....</b>	<b>268</b>
<b>5. Instalación de TOR.....</b>	<b>269</b>
<b>6. Comprobando la privacidad de la conexión .....</b>	<b>272</b>

## Capítulo XV

<b>lanGhost: Un backdoor con Raspberry Pi controlado mediante Telegram .....</b>	<b>277</b>
<b>1. Introducción.....</b>	<b>277</b>
<b>2. Descarga de lanGhost.....</b>	<b>278</b>
<b>3. Instalación de lanGhost .....</b>	<b>279</b>
Selección de la interfaz de red .....	279
Vinculación del bot de Telegram con lanGhost .....	279
Código de verificación .....	280
Configuración del arranque de lanGhost.....	281
<b>4. Inicio de lanGhost.....</b>	<b>281</b>
<b>5. Casos de uso de lanGhost.....</b>	<b>282</b>
<b>6. Ejemplos de usos con lanGhost .....</b>	<b>283</b>
Enumeración de dispositivos dentro de la LAN .....	284

---

Escaneo de los puertos TCP .....	285
Ataque Man in The Middle .....	286
Spoof DNS .....	288
Inyección de un fichero JavaScript .....	290
Desconexión de un nodo de Internet .....	291
Shell inverso .....	294
<b>Índice alfabético .....</b>	<b>297</b>
<b>Índice de imágenes .....</b>	<b>299</b>