

Índice

Prólogo	15
Capítulo I	
Zona de Confort	17
1. Hogar, “amargo” hogar	17
Por qué no dulce.....	18
2. El Router: Centro de Control de tus Comunicaciones.....	19
Función Principal	21
FTTH (Fibra hasta la Casa).....	23
VLANs y el 802.1Q	25
Ligero Paseo Lateral	28
Fin del Paseo	52
3. Respaldo a Internet con un buen Aliado para seguir en línea y no perder el “hilo”	52
Construir una pasarela en un PC	53
PC en rol de Switch: Pasarela en un Bridge.....	53
PC en rol de Router: Pasarela en un Gateway.....	58
Roles: Switch vs Router	61
Un Sistema de Router libre y transparente para el Aliado	62
Gargoyle: Un firmware para tu router inalámbrico.....	62
Puesta en marcha del Buffalo WZR-HP-G300NH2	63
De DD-WRT a Gargoyle.....	63
La misma WAN de (casi) siempre	68
La Contingencia Ayuda a salir “del paso”.....	76
Capítulo II	
Fisiología de la Red	77
1. Tomando a OSI como modelo	77
2. Wireshark y OSI: Una estrecha relación.....	83
El primer Chapuzón	84

Estadísticas: Protocolos y su Jerarquía	87
Chuleta Protocolaria.....	89
3. Protocolos de conexión de doble capa: Física & Enlace	96
Ethernet	97
10 en BASE a 5 o 2.....	97
10 o 100 o incluso 1000 en BASE a una T	98
Retro-Compatibilidad.....	100
¿Directo o Cruzado?.....	101
El Poder sobre Ethernet.....	102
El PoE casero en los 100BASE-T.....	102
El portero llamado 802.1X.....	104
Luz Fibrosa.....	106
4. Wi-Fi.....	107
El Despiece.....	109
5. Seguridad Wireless.....	111
WEP	111
802.11i.....	112
WPA con TKIP.....	112
ChopChop: El Picoteo.....	114
No más RC4.....	116
WPA con AES (WPAv2)	119
Seguridad Empresarial	121
KRACK - La Factura de la Fractura	121
WPS.....	124
HotSpot 2.0	127
Infraestructura del 802.11u	128
WPA parte 3	129
PMF: La nueva estrategia de defensa.....	130
1a Promesa: SAE.....	130
2a Promesa: 192-bit.....	131
3a Promesa: OWE.....	131
4a Promesa: Wi-Fi Easy Connect.....	132
DragonBlood: El rompedor de promesas.....	134
Downgradeando de WPA3 a WPA2.....	134
Downgradeando a grupos Inferiores-Inseguros	135
Ataques de canal lateral; De tiempo y caché	135
DragonDrain: Denegación de Servicio (DoS).....	136
6. Bluetooth	137
Los Perfiles Clásicos	138
El Low Energy o la Edad Moderna del Bluetooth	139
Roles de Conexionado.....	141

Intercambio de Datos	141
7. Seguridad Bluetooth.....	144
Estableciendo Conexión.....	144
Encasillando la Seguridad de la Azulada Caries.....	145
Debilidades Generales.....	147
DirtyTooth Hack.....	147
CrackLE	148
BtleJuice & GATTack	149
BlueBorne o los Odiosos 8.....	150
BleedingBIT.....	152
SweynTooth – La Familia Numerosa.....	155
BIAS (de escape).....	156

Capítulo III

Satélites que orbitan en un router157

1. ECO-Sistema.....	157
2. PreCheckeo: I&I, Identificación e Inventariado	160
Onboarding – Dando la bienvenida al nuevo Dispositivo	160
Parámetros que componen el ADN de un Dispositivo.....	167
Lo Primero - El Camino Fácil y Corto.....	171
Lo Segundo - El Camino Difícil y Largo.....	172
Level 1.....	173
Modelo vía Sistema	173
Modelo vía Ajena.....	176
Número de Serie y IMEI vía Sistema	177
Layer 2: ENLACE.....	178
MAC vía Sistema en Ethernet y Wi-Fi	178
MAC vía Ajena en Ethernet.....	181
MAC vía Ajena en Wi-Fi.....	185
MAC vía Sistema en Bluetooth	189
MAC vía Ajena en Bluetooth	189
Vlan ID vía Sistema.....	191
Vlan ID vía Ajena	192
Radio, Default Security y Default Network KEY vía Sistema.....	194
Radio y Default Security vía Ajena	195
Random vía Sistema	196
Random vía Ajena.....	196
Default SSID vía Sistema en Wi-Fi.....	197
Default SSID vía Ajena en Wi-Fi	197
WPS Default y WPS PIN vía Sistema	200
WPS Default vía Ajena.....	201

Layer 3: RED	203
Default IP e IPV6/Link-Local vía Sistema en Ethernet y Wi-Fi	203
Default IP, APIPA y IPV6/Link-Local vía Ajena en Ethernet	204
Default IP, APIPA y IPV6/Link-Local vía Ajena en Wi-Fi.....	212
Layer 7: APLICACIÓN	213
HOSTNAME vía Sistema en Ethernet y Wi-Fi	213
HOSTNAME vía Ajena en Ethernet y Wi-Fi	215
HOSTNAME, Firmware OS/Version, Classic/BLE vía Sistema en Bluetooth.....	220
HOSTNAME, Firmware OS/Version, Classic/BLE vía Ajena en Bluetooth	222
Top Level	222
Firmware OS/Version vía Sistema.....	223
Firmware OS/Version vía Ajena	224
Default User & Password vía Ajena	224
CVE vía Ajena	225
FINAL de los parámetros.....	229
3. Check-In de una Muestra por Categoría	230
Adaptando los Parámetros para sus Registros	230
Nodo de red – Router	231
Orden de Trabajo	231
Diagrama de Flujo	233
Pasando por “Caja”.....	234
Acechando al Dispositivo	234
Manual de Instrucciones Online de Adamo	234
Técnica vía Sistema	235
Técnica vía Ajena	237
Nodo de red – ONT.....	239
Venía “enCajado”.....	240
Un Distintivo más en Dispositivo.....	240
PC.....	241
Diagrama de Flujo	241
Los bajos del Dispositivo.....	242
Técnica vía Sistema	243
Técnica vía Ajena	244
Smartphone	244
¿Un móvil sin SIM sirve?.....	244
Diagrama de Flujo	246
Rebuscando en la “Incubadora”.....	247
DisPositivamente	247
Técnica vía Sistema	248
Técnica vía Ajena	252
Wearable – SmartWatch	252
Siempre en Hora y sin Internet	252

Diagrama de Flujo	253
Caja, Ideal para Regalo	253
Observando al Reloj	254
Técnica vía Sistema	255
Técnica vía Ajena	256
ANT+: De Diente Azul a Hormiga	257
Videoconsola – Handheld	257
Con tu Consola a cualquier Lugar	258
Diagrama de Flujo	258
Las Piezas del Rompecabezas	259
Técnica vía Sistema	261
Técnica vía Ajena	263
Disfrazándose de Joy-Con	266
El HomeBrew	272
Automatización del hogar/Domótica - Smart Wall Switch	273
La RED Eléctrica de Casa	274
Diagrama de Flujo	278
Caja Vistosa	279
Interruptor Electrónico	280
Técnica vía Sistema	280
Técnica vía Ajena	281
Almacenamiento – NAS	282
Menos es Más	283
RAID vs Backup	283
Diagrama de Flujo	286
Una Caja que enCaja	287
Técnica vía Ajena	288
Técnica vía Sistema	289
Surveillance - IP Camera	290
Tan Cerca y Lejos al mismo Tiempo	291
Diagrama de Flujo	293
Caja “Registradora”	295
Técnica vía Sistema	296
Técnica vía Ajena	298
Dispositivos de Trabajo – Impresora	300
El Cloud le da Alas	301
Wi-Fi Direct-O al cajón Desastre	302
Diagrama de Flujo	311
Caja Impresion-ada	313
Técnica vía Sistema	313
Técnica vía Ajena	318
Asistente de Voz Personal - Altavoz Inteligente	320
El secreto está en la Nube	320

Diagrama de Flujo	321
Caja de “Galleta”	322
La “Galleta”	323
Más que un Instructivo	324
Técnica vía Sistema	325
Técnica vía Ajena	326
Media/TV - Smart TV	330
Tres Dimensiones	331
Diagrama de Flujo	332
Sin Caparazón.....	334
Técnica vía Sistema	335
Técnica vía Ajena	342
Trazando Nuevas Rutas	347
Generic IoT – Tracker	353
Entre todos lo Encontraremos.....	353
Diagrama de Flujo	355
Fosforera o Caja de Cerillas	356
Las Cerillas (o cerilla solitaria).....	357
Técnica vía Ajena	358
Observaciones	359

Capítulo IV

Técnicas de Sniffing	361
1. Figonear conversaciones.....	361
2. Picando el Anzuelo	363
Hub vs Switch	363
3. El Anzuelo Envenenado	364
ARP Spoofing.....	364
Neighbor Advertisement Spoofing.....	366
4. Cautivo temporal en Pecera	367
Sniffing en el Propio Dispositivo	368
Test Access Port	368
Machine-in-the-Middle	371
Los 4 Pilares del Puente	372
Buscando los Tres Pies al Gato	378
HotSpot: El Punto “Caliente”.....	381
Port Mirroring: Los Espejos del Switch.....	382
Bluetooth: La suciedad de entre los Azules Dientes	384
5. Desvistiendo para la Auscultación	386
El Disfraz de los Datos.....	387

Confía en tus Progenitores	387
Asimétrico y Simétrico	392
Encriptación Asimétrica.....	392
Encriptación Simétrica.....	393
La Maestría de las Llaves.....	393
Aspecto e interpretación de SSLKEYLOGFILE	395
TLS 1.2 vs TLS 1.3	401
TLS 1.2	402
TLS 1.3	402
Interpretación del Diagrama/Esquema	406
QUIC-(K)	406
F12 – DevTools	409
PROXY Explícito.....	410
PROXY Implícito.....	416
Índice alfabético	423
Índice de imágenes	435
Otros libros publicados.....	445

