

Índice

Introducción	11
Capítulo I	
Alternativas para la navegación anónima y privacidad en Internet.....	13
1.1 ¿Por qué debo preocuparme por mi privacidad en Internet? No tengo nada que ocultar	13
1.1.1 Seguimiento, vigilancia y herramientas para proteger la privacidad de los usuarios	14
1.1.1.1 Políticas de Privacidad.....	15
1.1.1.2 Cookies	15
1.1.1.3 Elementos persistentes de HTML5.....	17
1.1.1.4 Identificación del navegador.....	18
1.1.1.5 Dirección IP y geolocalización	18
1.1.1.6 Registros de actividad.....	19
1.1.1.7 Redes sociales.....	19
1.1.1.8 Servicios de Google.....	22
1.1.1.9 Supercookies o cookies persistentes.....	24
1.1.1.10 Descuidos y malas prácticas	26
1.1.2 Herramientas para impedir la vigilancia y seguimiento de usuarios.....	28
1.1.2.1 Buscadores.....	28
1.1.2.2 Configuración de la privacidad en navegadores web	29
1.1.2.3 Navegación segura.....	34
1.1.2.4 HTTPS Everywhere.....	35
1.1.2.5 Políticas HSTS (Http Strict Transport Security).....	37
1.1.2.6 Servicios VPN.....	41
1.1.2.7 Servidores proxy anónimos	43
1.1.2.8 Complementos en navegadores web.....	44
1.1.2.9 Privacy Badger.....	47
1.1.2.10 AdBlock Plus	48
1.1.2.11 NoScript.....	48
1.1.2.12 BetterPrivacy	48
1.1.2.13 Greasemonkey	49
1.2 Redes anónimas y la web profunda.....	49
1.2.1 La web profunda	49



1.2.2 Darknets	51
1.2.3 ¿Privacidad o ciberdelincuencia?	52

Capítulo II

I2P (Invisible Internet Project)55

2.1 Introducción55

2.1.1 Instalación de I2P	56
2.1.2 Servicios ocultos en I2P	58
2.1.2.1 Servicios ocultos para comenzar a descubrir la web profunda de I2P.....	61

2.2 Arquitectura66

2.2.1 Túneles	66
2.2.2 Preprocesamiento de Mensajes I2NP y mensajes Garlic.....	68
2.2.3 Base de datos de la red (NetDB).....	71
2.2.4 Protocolos y capas.....	73
2.2.4.1 Capa de Aplicación	74
2.2.4.2 Capa de Cifrado Garlic	74
2.2.4.3 Capa de Túneles	74
2.2.4.4 Capa de Transporte I2P.....	75
2.2.4.5 Capa de Transporte y capa IP	76

2.3 Gestión de servicios y complementos en I2P76

2.3.1 Clientes y servicios en I2P	79
2.3.1.1 Creación de servicios ocultos y túneles cliente con I2PTunnel	84
2.3.1.2 Servicio Oculito HTTP (Eepsite).....	84
2.3.1.3 Otros tipos de servicios ocultos	87

2.4 Acceso programático.....90

2.4.1 SAM (Simple Anonymous Messaging)	90
2.4.2 BOB (Basic Open Bridge)	93
2.4.3 Streaming Library	98

Capítulo III

FreeNET.....103

3.1 Introducción103

3.1.1 Instalación de Freenet	104
3.1.2 Servicios ocultos en Freenet.....	108
3.1.2.1 Servicios ocultos para comenzar a descubrir la web profunda de Freenet.....	108

3.2 Arquitectura111

3.2.1 Darknets en Freenet.....	111
3.2.2 Almacenamiento de datos: Datastore en Freenet	113
3.2.3 Funcionamiento de las claves en Freenet.....	115



3.2.4 Enrutamiento en Freenet	118
3.3 Gestión de servicios y complementos en Freenet	119
3.3.1 Frost.....	120
3.3.2 JSite	121
3.3.3 Complementos en Freenet.....	123
3.3.3.1 Web of Trust (complemento oficial)	124
3.3.3.2 Floghelper (complemento oficial).....	125
3.3.3.3 Freemail (complemento oficial).....	126
3.4 Acceso programático.....	127
3.4.1 Desarrollo de complementos en Freenet.....	127
3.4.1.2 Elementos de la API Java de Freenet.....	130
3.4.1.3 Creación de un complemento utilizando la API de Freenet	131
3.4.2 Text Mode Client Interface (TMCI).....	133
3.4.2.1 Tipos de comandos en TMCI.....	135

Capítulo IV

Tor (The Onion Router).....143

4.1 Introducción	143
4.1.1 Instalación y configuración de una instancia de Tor	143
4.1.1.1 Tor Browser	144
4.1.1.2 Instalación de una instancia de Tor.....	144
4.1.2 Instalación de Privoxy con Tor.....	146
4.1.3 Instalación de Polipo con Tor.....	146
4.1.4 La web profunda de Tor	149
4.1.4.1 Servicios ocultos para comenzar a descubrir la web profunda de Tor.....	150
4.2 Arquitectura	158
4.2.1 Repetidores.....	158
4.2.2 Descriptores.....	160
4.2.3 Circuitos	162
4.2.4 Servicios ocultos	163
4.2.4.1 Instalación y configuración de un servicio oculto	164
4.2.4.2 Pentesting contra servicios ocultos.....	169
4.2.4.3 Personalización de direcciones onion.....	176
4.2.5 Puentes	179
4.2.5.1 Pluggable Transports en Tor	183
4.2.6 Autoridades de directorio	186
4.2.6.1 Proceso de votación y generación de consenso	187
4.2.6.2 Caches de directorio	189
4.2.6.3 Instancias cliente de Tor	190
4.3 Gestión de servicios y complementos en Tor	192



4.3.1 Ejecución de aplicaciones por medio de Tor (Torify)	192
4.3.1.1 TorSocks	192
4.3.1.2 tor-resolve	194
4.3.1.3 ProxyChains	194
4.3.1.4 TorTunnel	195
4.3.1.5 Cifrado punto a punto con SSH	197
4.3.2 Evitando DNS Leaks y fugas de información	199
4.3.3 Protocolo de control de Tor	202
4.3.3.1 Uso de ARM para monitorizar una instancia de Tor	202
4.3.4 TAILS (The Amnesic Incognito Live System)	206
4.3.5 Directivas de configuración	209
4.3.5.1 Directivas relacionadas con caches y autoridades de directorio	209
4.3.5.2 Directivas relacionadas con repetidores	211
4.3.5.3 Directivas relacionadas con clientes	213
4.4 Acceso programático	216
4.4.1 Stem	217
4.4.1.1 Ejemplos del uso de Stem	217
4.4.2 TxTorCon	220
4.4.2.1 Creación de servicios ocultos con TxTorCon	221
Capítulo V	
Otras soluciones enfocadas a la privacidad y el anonimato	225
5.1 GNUnet	225
5.1.1 Instalación	226
5.1.2 Publicación y consulta de ficheros en GNUNet	228
5.2 Lantern	230
5.3 YaCy	231
5.5 Hyperboria	234
5.5.1 Instalación de CJDNS	234
5.6 Osiris SPS	236
Índice alfabético	239
Índice de imágenes	241

