

Índice

Prólogo	9
Capítulo I: Introducción.....	11
1. Un poco de historia	11
2. ¿Por qué Asterisk?.....	12
3. ¿Por qué este libro?	13
4. Diferentes escenarios	14
5. Protocolos para la VoIP	17
6. Protocolo SIP.....	21
7. Códecs.....	27
Capítulo II: Test de penetración	31
1. Recopilación de información: Footprinting	32
1.1. Numeración y proveedores	32
1.2. Administradores	35
1.3. Usuarios	36
2. Enumeración: Fingerprinting	36
2.1. Enumeración de extensiones.....	54
3. Análisis: Búsqueda de vulnerabilidades.....	57
3.1. Identificación de servicios	57
4. Explotación	58
4.1. Ataques contra dispositivos	60
4.2. Prevención	60



Capítulo III: Ataques en redes locales	65
1. Redes inalámbricas	66
2. Ataques ‘Man in the middle’	68
3. Analizando capturas de red	71
4. Prevención.....	79
Capítulo IV: Buscando objetivos	81
1. Búsquedas a través de Google	82
2. Búsquedas a través de Shodan	83
Capítulo V: Otros ataques	89
1. Problemas en la configuración de usuarios	89
2. Problemas en la configuración de contextos	91
3. Problemas en la configuración de IVRs	100
4. Problemas en la configuración de planes de llamada.....	102
5. Configuración de dominios	104
6. Sistemas de Click2Call	104
7. Escuchas ilegales (Eavesdropping)	108
7.1. Escuchas en tiempo real.....	109
7.2. Grabación de conversaciones	110
8. Interceptación y modificación de conversaciones.....	113
9. Servicios TFTP.....	124
10. Ataques de denegación de servicio	125
11. Buscando nuevas vulnerabilidades	130
Capítulo VI: Problemas de los Front-end prediseñados	133
1. Análisis de una FreePBX	134
1.1. Algunos conceptos sobre la VoIP.....	138



1.2. Consiguiendo acceso al sistema.....	140
1.3. Analizando los servicios	149
1.4. Troyanizando el Asterisk	155
2. Análisis de un Elastix	159
3. Análisis de un Trixbox	161
4. Escalada de privilegios en FreePBX, Elastix y Trixbox	162
5. Conclusiones	165
Capítulo VII: Fraudes a través de VoIP.....	167
1. Vishing: Phising a través de VoIP	168
2. SPIT: Spam telefónico	169
3. Montando una centralita pirata	170
4. Realizando llamadas anónimas a través de Tor.....	172
Capítulo VIII: Restringiendo y monitorizando el sistema	179
1. Restricción de destinos.....	179
2. Restricción de horarios.....	182
3. Restricción de consumo	183
4. Monitorizando nuestro sistema	185
4.1. Monitorización manual.....	185
4.2. Monitorización automática	186
Capítulo IX: Repaso de algunos bugs	191
1. Asterisk Manager User Unauthorized Shell Access.....	191
2. Asterisk Remote Crash Vulnerability in SIP channel driver	194
3. All your Calls Are Still Belong to Us.....	195
4. FreePBX / Elastix Recordings Interface Remote Code Execution Vulnerability.....	196



Referencias	199
RFCs	199
Documentación sobre la VoIP	199
Servidores de VoIP y distribuciones	199
Herramientas de interés	200
Blogs de interés.....	201
Información.....	202
Avisos de seguridad y publicación de exploits	202
Otros enlaces de interés	202
Bibliografía	203
Libros.....	203
Artículos y definiciones	203
Índice alfabético	207
Índice de imágenes	213
Libros publicados.....	217
Contacta con Informática 64.....	224

