

Índice

Prólogo 1	11
------------------------	-----------

Prólogo 2	13
------------------------	-----------

Capítulo I:

Introducción	15
---------------------------	-----------

1. Un poco de historia	15
2. ¿Por qué Asterisk?.....	16
3. ¿Por qué este libro?	17
4. Diferentes escenarios	19
5. Protocolos para la VoIP	21
6. Protocolo SIP.....	25
7. Códecs	31
8. Problemas en la VoIP	34

Capítulo II:

Test de penetración	37
----------------------------------	-----------

1. Recopilación de información: Footprinting	38
1.1. Numeración y proveedores	38
1.2. Administradores.....	41
1.3. Usuarios	42
2. Enumeración: Fingerprinting	42
2.1. Enumeración de extensiones.....	60



3. Análisis: Búsqueda de vulnerabilidades.....	63
3.1. Identificación de servicios	63
4. Explotación	65
4.1. Ataques contra dispositivos	66
4.2. Prevención	67

Capítulo III:

Ataques en redes locales 71

1. Redes inalámbricas	72
2. Ataques ‘Man in the middle’	74
3. Analizando capturas de red	77
4. Prevención.....	85

Capítulo IV:

Buscando objetivos..... 87

1. Búsquedas a través de Google	88
2. Búsquedas a través de Shodan	89

Capítulo V:

Otros ataques..... 95

1. Problemas en la configuración de usuarios	95
2. Problemas en la configuración de contextos	97
3. Problemas en la configuración de IVRs.....	106
4. Problemas en la configuración de planes de llamada.....	108
5. Configuración de dominios	110
6. Sistemas de Click2Call	110
7. Escuchas ilegales (Eavesdropping)	114
7.1. Escuchas en tiempo real.....	115
7.2. Grabación de conversaciones	116



8. Interceptación y modificación de conversaciones.....	119
9. Servicios TFTP.....	130
10. Ataques de denegación de servicio	131
11. Buscando nuevas vulnerabilidades	136

Capítulo VI:

Problemas de los Front-end prediseñados 139

1. Análisis de una FreePBX	140
1.1. Algunos conceptos sobre la VoIP.....	144
1.2. Consiguiendo acceso al sistema.....	146
1.3. Analizando los servicios	154
1.4. Troyanizando el Asterisk	161
2. Análisis de un Elastix	165
3. Análisis de un Trixbox	167
4. Escalada de privilegios en FreePBX, Elastix y Trixbox	168
5. Conclusiones	171

Capítulo VII:

Fraudes a través de VoIP..... 173

1. Vishing: Phising a través de VoIP	174
2. SPIT: Spam telefónico	175
3. Montando una centralita pirata	176
4. Realizando llamadas anónimas a través de Tor.....	178

Capítulo VIII:

Restringiendo y monitorizando el sistema 185

1. Restricción de destinos.....	185
2. Restricción de horarios.....	188
3. Restricción de consumo	189



4. Monitorizando nuestro sistema	191
4.1. Monitorización manual	191
4.2. Monitorización automática	192

Capítulo IX:

Repaso de algunos bugs 197

1. Asterisk Manager User Unauthorized Shell Access.....	197
2. Asterisk Remote Crash Vulnerability in SIP channel driver	200
3. All your Calls Are Still Belong to Us.....	201
4. FreePBX / Elastix Recordings Interface Remote Code Execution Vulnerability.....	202

Referencias 205

RFCs	205
Documentación sobre la VoIP	205
Servidores de VoIP y distribuciones	205
Herramientas de interés	206
Blogs de interés.....	207
Información.....	208
Avisos de seguridad y publicación de exploits	208
Otros enlaces de interés	208

Bibliografía 209

Libros.....	209
Artículos y definiciones	209

Índice alfabético 213

Índice de imágenes 219

