

Índice de contenido

Introducción	XIX
1 Conceptos IP	1
El modelo de Internet TCP/IP	2
Empaquetado (más allá del papel o el plástico)	4
Direcciones	9
Puertos de servicio	13
Protocolos IP	14
Sistema de nombres de dominio	16
Enrutamiento: cómo llegamos allí desde aquí	17
Resumen	19
2 Introducción a TCPdump y al Protocolo de control de transmisión (TCP)	21
TCPdump	22
Introducción a TCP	28
El fracaso de TCP	34
Resumen	38
3 Fragmentación	39
Teoría de la fragmentación	39
Fragmentación malintencionada	48
Resumen	51
4 ICMP	53
Teoría ICMP	53
Técnicas de correspondencia	56
Actividad ICMP normal	61
Actividad ICMP malintencionada	65
Bloquear o no bloquear	71
Resumen	73
5 Estímulo y respuesta	75
Lo esperado	76
Desviaciones del protocolo	82
Resumen del comportamiento esperado y las desviaciones del protocolo	84

VI Índice de contenido

Estímulos anormales	84
Estímulo no convencional, respuesta de identificación del sistema operativo	88
Resumen	93
6 DNS	95
De vuelta a los fundamentos: teoría DNS	96
Búsquedas inversas	103
Cómo utilizar DNS para el reconocimiento	107
Cómo tantear respuestas DNS	111
Resumen	114
7 Ataque Mitnick	115
Explotación de TCP	115
Cómo detectar el ataque Mitnick	126
Sistemas de detección de intrusos basados en redes	127
Sistemas de detección de intrusos basados en <i>hosts</i>	129
Cómo evitar el ataque Mitnick	131
Resumen	132
8 Introducción a los filtros y a las firmas	133
Normativa de filtrado	133
Firmas	134
Filtros utilizados para detectar eventos de interés	135
Ejemplos de filtros	136
Ejemplo de filtro Snort	147
Problemas de normativa relacionados con la utilización de filtros	150
Resumen	153
9 Problemas de arquitectura	155
Eventos de interés	156
Límites de la observación	156
Paradigma de la fruta que cuelga	158
Detecciones limitadas por factores humanos	159
Severidad	161
Contramedidas	164
Cálculo de la severidad	164
Ubicación de los sensores	167
Empujar-tirar	170
Consola de analista	171
Detección de intrusos basada en red o en <i>host</i>	176
Resumen	177
10 Interoperatividad y correlación	179
Múltiples soluciones trabajando juntas	180
Soluciones de interoperatividad IDS comerciales	184
Correlación	185
Bases de datos SQL	196
Resumen	201
11 Soluciones de detección de intrusos basadas en red	203
Snort	203
Herramientas comerciales	204
Sistemas basados en UNIX	209
GOTS	211
Evaluación de los sistemas de detección de intrusos	214
Resumen	217

12 Tendencias futuras	219
Amenaza creciente.....	220
Herramientas mejoradas.....	221
Búsqueda de objetivos mejorada.....	221
Código móvil.....	222
Puertas trampa.....	222
Compartición, la herencia del Y2K.....	225
Confianza interna.....	228
Respuesta mejorada.....	230
Volvemos a visitar la industria de los virus.....	231
ID basado en hardware.....	231
Defensa en profundidad.....	232
ID basado en programa.....	233
Audidores inteligentes.....	234
Resumen.....	234
13 <i>Exploits</i> y exploraciones para aplicar <i>exploits</i>	235
Falsos positivos.....	235
<i>Exploits</i> IMAP.....	244
Exploraciones para aplicar <i>exploits</i>	248
<i>Exploit</i> único, portmap.....	252
Resumen.....	260
14 Denegación de servicio	261
Ejemplos de denegación de servicio por fuerza bruta.....	261
Presas elegantes.....	266
nmap 2.53.....	270
Ataques de denegación de servicio distribuida.....	271
Resumen.....	274
15 Detección de la reunión de información	277
Correspondencia de red y de <i>host</i>	278
Rastros específicos de NetBIOS.....	288
Ataques sigilosos.....	290
Medición del tiempo de respuesta.....	295
Los virus como recolectores de información.....	298
Resumen.....	301
16 Problemas con las RPC	303
portmapper.....	303
dump es un componente esencial de rpcinfo.....	306
Ataques que acceden directamente a un servicio RPC.....	308
El árbol grande.....	311
Análisis bajo el fuego.....	312
Un último ejemplo, rpc.ttdbserverd.....	316
¡Oh, nmap!.....	316
Resumen.....	319
17 Filtros para detectar, filtros para proteger	321
Los mecanismos de escritura de filtros TCPdump.....	322
Enmascaramiento de bit.....	323
Filtros IP de TCPdump.....	327
Filtros TCPdump de UDP.....	329
Filtros TCPdump de TCP.....	331
Resumen.....	335

18 Compromiso del sistema	337
Nochebuena de 1998	338
¿Dónde hacen la compra los atacantes?	351
Red de comunicaciones	354
Anonimato	356
Resumen	357
19 A la caza del timex	359
Los rastros	359
Comienza la caza	362
Y2K	368
Orígenes encontrados	372
Descubrimientos varios	373
Lista de verificación de resumen	376
Epílogo y propósito	377
Resumen	378
20 Problemas de organización	379
Modelo de seguridad de organización	379
Definición de riesgo	384
Riesgo	385
Definición de la amenaza	390
La administración del riesgo va orientada por el dinero	395
¿Cómo de arriesgado es un riesgo?	395
Resumen	397
21 Respuesta manual y automática	399
Respuesta automática	400
<i>Honeypot</i>	406
Respuesta manual	408
Resumen	416
22 Caso de empresa para la detección de intrusos	417
Primera parte: problemas de dirección	419
Segunda parte: amenazas y vulnerabilidades	423
Tercera parte: negociaciones y solución recomendada	428
Repeticón del Resumen Ejecutivo	433
Resumen	434
Índice alfabético	435