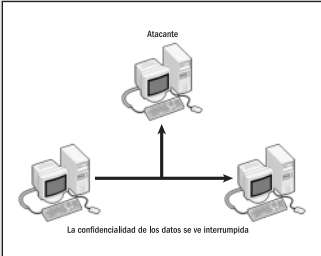


CONTENIDO

Sobre el autor	4
Prólogo	5
El libro de un vistazo	8
Información complementaria	9
Introducción	15
Capítulo 1	
PILARES BÁSICOS	
¿Qué es la seguridad?	18
Confidencialidad	18
Integridad	18
Disponibilidad	18
Autenticidad	18
¿Qué queremos proteger?	20
Importancia de los elementos	21
 <p>La confidencialidad de los datos se ve interrumpida</p>	
¿De qué nos protegemos?	24
Factores humanos	25
Factores no humanos	29
Resumen	29
Actividades	30
Capítulo 2	
POLÍTICA DE SEGURIDAD	
Creación de un plan	32
Responsabilidades	34
Riesgos	35
Procedimientos	38
¿Quién utilizará el recurso?	39
¿Cuál es el empleo de cada recurso?	39

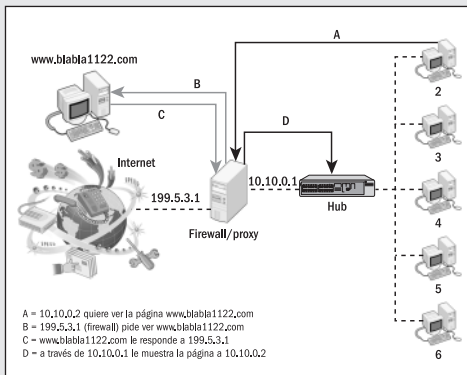
¿Cuáles son las obligaciones de los usuarios?	41
¿Quién aprueba el uso de un recurso?	42
	
El administrador	44
Incidentes	44
Estrategias de respuestas	45
Problemas comunes	46
Modelos de políticas	46
Modelo Bell-Lapadula (BLP)	46
Modelo de Clark-Wilson	47
Resumen	47
Actividades	48
Capítulo 3	
DISEÑO DE RED	
Redes seguras	50
Topologías	51
	

Protocolos de enrutamiento	57
¿Qué es un DMZ?	59
Proteger los dispositivos	60
VPN (red privada virtual)	61
¿Por qué una VPN?	61
Tipos de VPN	61
Seguridad	63
Resumen	63
Actividades	64

Capítulo 4

DISPOSITIVOS DE SEGURIDAD

Filtrado	66
Filtrado de paquetes	66
Plataformas	71

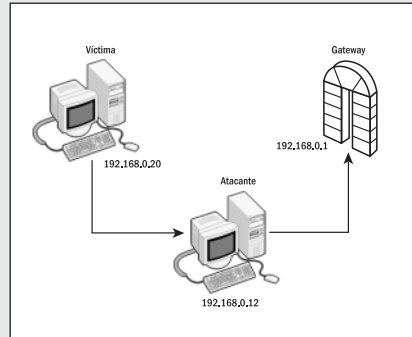


IDS	75
IPS	79
Resumen	81
Actividades	82

Capítulo 5

AMENAZAS

Introducción	84
Ataques Internos (AI)	84
Métodos de prevención	87
Ataques Externos (AE)	91
IP Spoofing	92
AXFR	95
Amenazas Humanas (AH)	98

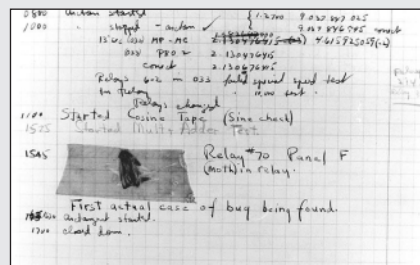


Resumen	101
Actividades	102

Capítulo 6

VULNERABILIDADES

¿Qué es una vulnerabilidad?	104
Ejemplo 1: Celulares	105
Ejemplo 2: Alarmas	105
Ejemplo 3: Telefonía	106
Grace Murray Hopper (1906-1992)	107



Tipos de vulnerabilidades	108
Buffer overflows	108
Ataques DoS	111
Exploits	115
Resumen	119
Actividades	120

Capítulo 7

SEGURIDAD FÍSICA

Introducción	122
Los accesos	122
Datacenter	122

Seguridad contra desastres	123
Electricidad	123
Incendios	124
Temperatura	125
Backups	125
Redundancia	126
¿Qué es warchalking?	127



Acceso físico al hardware	127
¿Cerraduras o cerrablandas?	128
Cámaras de seguridad	129
Ventanas	129
¿Qué es trashing?	129
¿Qué son los keycatchers?	130
Bocas de red	130
Datos técnicos	130
Pen drive	131
Resumen	131
Actividades	132

Capítulo 8

HACKERS

Historia	134
Internet	135
Vinton Cerf	136
Robert Morris	137
Hackers telefónicos	139
Esas cajas de colores	140
Joe Engressia	142
John Draper	143

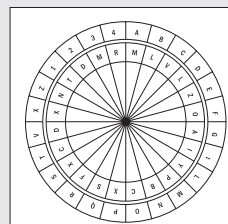


Oak Toebark y Berkeley Blue	144
Kevin Poulsen	145
Hackers, en la actualidad	145
Kevin Mitnick	148
El ataque Mitnick	153
Identificación	154
Verificación	156
Ataque	157
Fin de la técnica	158
Resumen	159
Actividades	160

Capítulo 9

CRIPTOGRAFÍA

Introducción	162
La importancia de la codificación	163
Un poco de historia	164
Métodos antiguos	165
La escítala	165
Método Polybios	165
El método de César	166
El disco de Alberti	167



Criptografía moderna	168	NMAP	197
Criptografía simétrica	169	Auditoría	202
Criptografía asimétrica	170	El auditor	202
Algoritmo Rivest, Shamir y Adelman (RSA)	171	Diferencias	202
Propiedades del algoritmo RSA	171	Valor agregado	203
Funcionamiento	172	Análisis completo	204
Diffie y Hellman	173	Análisis por Web	209
PGP	173	Pen Test	211
Instalación	174	Herramientas útiles	214
Anillos y certificados	175	Resumen	221
Firma digital	176	Actividades	222
Importancia	178		
Colisiones	179	Apéndice A	
Certificados digitales	180	CLAVES DE FÁBRICAS	
Validez	182	Listas	224
Emisión	183	Claves de fábrica	224
Tipos de certificados	184	Lista de puertos de las aplicaciones	266
Protocolos de seguridad	185	Mensajería instantánea	
Secure Socket Layer	185	y videoconferencia	266
S-HTTP	186		
Transport Layer Security	187	Apéndice B	
Secure Electronic Transaction	187	ISO 17799	
Resumen	189	Introducción	276
Actividades	190	Política de seguridad	279
		Organización	279
		Acceso por parte de terceros	280
		Tipos de acceso	280
		Contratistas en situ	281
		Seguridad del personal	281
		Acuerdo de no confidencialidad	281
		Capacitación del usuario	282
		Comunicación de incidentes	282
		Documentación	282
		Cambios en las operaciones	283
		Separación de funciones	284
		Aprobación	284
		Software malicioso (malware)	285
		Seguridad de la documentación	286
		Comercio electrónico	286
		Control de acceso	287

Capítulo 10

HERRAMIENTAS

Introducción	192
Netcat	192
Escaneadores de puertos	195

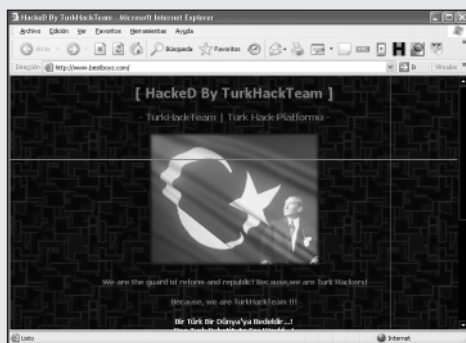


Política de control de acceso	287
Monitoreo	290
Registro	290
Monitoreo	290
Revisión	291
Dispositivos móviles	292
Trabajo remoto	292
Administración de claves criptográficas	293
Cumplimiento	294
Derecho de propiedad intelectual	294
Protección de datos	295
Prevención	295
Regulación criptográfica	295
Revisión de la política de seguridad	296

Apéndice C

PREGUNTAS FRECUENTES

Dudas, problemas y curiosidades	298
1. ¿Es posible hackear un correo electrónico?	298
2. ¿Es posible hackear una página?	299



3. ¿Es posible entrar en la NASA, el Pentágono, etc.?	300
4. ¿Cómo hacemos para ser un hacker?	301
5. ¿Podemos comprar cosas con tarjetas de otros?	301
6. ¿Podemos llamar gratis?	301
7. ¿Firewall de soft o de hard?	302
8. La auditoría ¿es necesaria?	302
9. Una política de seguridad ¿es necesaria?	302
10. ¿Es necesario saber programar?	303
11. Los exploits ¿son legales?	303
12. ¿Linux o Windows?	303

Servicios al lector

Seguridad Informática	306
Antivirus Online	306
Antitrojanos/spyware online	306
Escáneres de puertos online	306
Foros de seguridad	306
Índice temático	307