

Ciberseguridad

Manual práctico

José Manuel Ortega Candel

Ortega Candel, José Manuel, autor

Ciberseguridad : manual práctico / José Manuel Ortega Candel. -- Primera edición. --
Bogotá : Ecoe Ediciones ; Madrid : Ediciones Paraninfo, 2024.
335 páginas. -- (Computación y tecnología de la información. Seguridad informática)

Incluye datos curriculares del autor.

ISBN 978-958-503-839-4 -- 978-958-503-840-0 (e-book)

1. Seguridad informática - Manuales 2. Internet - Medidas de seguridad - Manuales 3.
Protección de datos - Manuales

CDD: 005.8 ed. 23

CO-BoBN- a1133895



Área: *Computación y tecnología de la información*

Subárea: *Seguridad informática*

ECOE
EDICIONES



Paraninfo

© José Manuel Ortega Candel

© Ediciones Paraninfo, SA
info@paraninfo.es
www.paraninfo.es
Teléfono: (+34) 914 463 350
Calle José Abascal 41,
Oficina 701. 28003
Madrid, España

© Ecoe Ediciones S.A.S.
info@ecoediciones.com
www.ecoediciones.com
Carrera 19 # 63 C 32
Teléfono: (+57) 321 226 46 09
Bogotá, Colombia

Primera edición: Bogotá, enero del 2024

ISBN: 978-958-503-839-4
e-ISBN: 978-958-503-840-0

Directora editorial: Ana María Rueda G.
Coordinadora editorial: Paula Bermúdez B.
Editora de adquisiciones: Alejandra Cely R.
Carátula: Wilson Marulanda Muñoz
Impresión: Xpress Estudio Gráfico y Digital
Carrera 69 H # 77 - 40

*Prohibida la reproducción total o parcial por cualquier medio
sin la autorización escrita del titular de los derechos patrimoniales.*

Impreso y hecho en Colombia - Todos los derechos reservados

Contenido

1. INTRODUCCIÓN A LA CIBERSEGURIDAD	1
1.1. Diferencia entre seguridad de la información y ciberseguridad	2
1.2. Objetivos de la ciberseguridad	3
1.2.1. Confidencialidad	4
1.2.2. Integridad	5
1.2.3. Disponibilidad	7
1.2.4. Resumen	8
1.3. Personas y roles en ciberseguridad	8
1.3.1. Profesionales de la ciberseguridad	9
1.3.2. Gerente de seguridad de la información	11
1.3.3. Gobierno de la ciberseguridad	12
1.4. Dominios de la ciberseguridad	13
1.4.1. Conceptos de ciberseguridad	14
1.4.2. Principios de arquitectura de ciberseguridad	14
1.4.3. Seguridad de redes, sistemas, aplicaciones y datos	15
1.4.4. Respuesta a incidentes	15
1.4.5. Dominios de seguridad según el estándar ISO 27000	15
1.5. Gestión de riesgos y controles de ciberseguridad	16
1.5.1. Gestión de riesgos	17
1.5.2. Controles de ciberseguridad	18
1.6. <i>Frameworks</i> de ciberseguridad	21
1.6.1. <i>Framework</i> de ciberseguridad NIST	21
1.6.2. Controles de ciberseguridad NIST	24
1.6.3. Controles de ciberseguridad CIS	26
Enlaces web de interés	27
Actividades finales	28
2. SEGURIDAD EN LA NUBE	31
2.1. Introducción a la computación en la nube (<i>cloud computing</i>)	32
2.2. Modelos de servicios en la nube (IaaS, PaaS, SaaS)	34
2.2.1. <i>Software as a service</i> (SAAS)	35
2.2.2. <i>Platform as a service</i> (PAAS)	36
2.2.3. <i>Infrastructure as a service</i> (IAAS)	37
2.3. Seguridad en la nube	38
2.3.1. Riesgos de computación y aplicaciones en la nube	42



2.4. Cifrado de la información en la nube	43
2.4.1. Tipos de cifrado	44
2.4.2. El cifrado en la nube: proveedor y cliente	45
2.5. Herramientas de cifrado de archivos	46
2.5.1. Boxcryptor	47
2.5.2. Cryptomator	47
2.5.3. Spideroak	48
2.5.4. Tresorit	48
2.5.5. Nextcloud	49
2.5.6. Owncloud	51
2.5.7. Otras soluciones	52
2.5.8. Conclusiones sobre la nube privada	53
2.6. Uso de certificados de forma segura	53
2.6.1. El protocolo SSL	54
2.6.2. Ejemplo de certificado seguro	55
2.6.3. Let's Encrypt	56
Enlaces web de interés	57
Actividades finales.	58

3. SEGURIDAD EN INTERNET

61

3.1. Tipos de amenazas y ataques en internet	62
3.1.1. Ciberamenazas	63
3.1.2. Principales amenazas de ciberseguridad	64
3.2. Introducción al <i>malware</i> y tipos	66
3.2.1. Troyanos	68
3.2.2. Clasificación de los <i>rootkits</i>	69
3.2.3. <i>Keyloggers</i> y <i>screen scrapers</i>	70
3.2.4. <i>Botnets</i>	70
3.2.5. Identificación de <i>malware</i>	72
3.3. Amenazas persistentes avanzadas (APT) y ataques dirigidos	74
3.3.1. Métodos de infección	75
3.3.2. Ataques de denegación de servicio	78
3.3.3. Ataques de correo electrónico y <i>cookies</i>	80
3.3.4. Ataques de DNS (sistema de nombres de dominio)	81
3.3.5. <i>Ransomware</i>	83
3.4. Protección de los sistemas frente a las amenazas.	85
3.4.1. Protección de las infraestructuras críticas	87
3.4.2. Protección frente a ataques DDoS.	88
3.4.3. Protección frente a ataques DNS.	89
3.5. Protección frente a amenazas persistentes avanzadas	91
3.6. Protección frente a <i>malware</i> (virus, troyanos, <i>spyware</i> , <i>rootkits</i>).	93
3.6.1. Uso de un antivirus.	95
3.6.2. Protección <i>antibotnet</i>	95
3.6.3. Detección de <i>malware</i> en Linux con LMD (Linux Malware Detect).	96
Enlaces web de interés	98
Actividades finales.	99

4. PRIVACIDAD EN INTERNET

101

4.1. Introducción a la privacidad	102
4.2. Privacidad de información en la nube	104
4.2.1. VPN (red privada virtual).	104
4.2.2. Proveedores VPN	106
4.2.3. OpenVPN	107



4.3. Privacidad en dispositivos IoT (<i>Internet of Things</i>)	108
4.3.1. Tendencias de privacidad en IoT en las organizaciones.	110
4.4. Privacidad en los navegadores.	111
4.4.1. Herramientas para el control de las <i>cookies</i>	112
4.5. Conexión con la red Tor	115
4.5.1. Navegador Tor Browser	116
4.5.2. Navegación anónima en la red Tor	119
4.6. Navegadores y buscadores alternativos	120
4.6.1. Brave.	121
4.6.2. DuckDuckGo	122
4.6.3. Buscadores alternativos.	124
Enlaces web de interés	127
Actividades finales.	128

5. SEGURIDAD EN APLICACIONES WEB

131

5.1. Metodología OWASP	132
5.2. Ataques en aplicaciones web	133
5.2.1. Vectores de ataque	136
5.2.2. XSS (<i>Cross-Site Scripting</i>).	137
5.2.3. CSRF (<i>Cross-Site Request Forgery</i>).	142
5.2.4. Seguridad en las redirecciones	143
5.2.5. Autenticación y manejo de sesiones	144
5.3. SQL Injection: parametrización de las consultas en bases de datos	147
5.3.1. Introducción a SQL injection	147
5.3.2. Problemas que pueden causar este tipo de ataques.	147
5.3.3. Ejemplo de SQL injection	148
5.3.4. Escapar los caracteres especiales utilizados en las consultas SQL	150
5.3.5. Uso de sentencias preparadas parametrizadas.	151
5.4. Herramientas para capturar las peticiones en aplicaciones web	152
5.4.1. OWASP ZAP.	152
5.4.2. BurpSuite	160
5.4.3. Fiddler	162
5.5. sqlmap	163
Enlaces web de interés	168
Actividades finales.	169

6. DESARROLLO SEGURO DE APLICACIONES

173

6.1. Introducción al desarrollo seguro	174
6.2. Ciclo de vida de desarrollo de <i>software</i> (SDLC).	175
6.3. Desarrollo y operaciones TI (DevOps).	176
6.3.1. DevSecOps.	178
6.3.2. Seguridad por diseño	181
6.4. Requisitos de seguridad en las aplicaciones.	181
6.5. Arquitectura segura en las aplicaciones.	183
6.5.1. Autenticación	183
6.5.2. Gestión de sesiones.	184
6.5.3. Control de acceso	184
6.5.4. Validación de entradas	185
6.5.5. Codificación de salida y rutinas de escape	185
6.5.6. Criptografía.	185
6.5.7. Gestión de errores y <i>logging</i>	186
6.5.8. Protección de datos.	186
6.5.9. Seguridad en las comunicaciones	187



6.5.10. Seguridad en el protocolo HTTPS	187
6.5.11. Codificación segura en las aplicaciones	188
6.6. Herramientas de pruebas de seguridad	188
6.6.1. OSSTMM (<i>Open Source Security Testing Methodology Manual</i>)	189
6.6.2. Auditorías de seguridad del código	189
6.6.3. Revisión de código automatizada	190
6.6.4. Análisis estático seguro de código (SAST)	191
6.6.5. Análisis de dependencias	193
6.6.6. Pruebas dinámicas de seguridad (DAST)	194
6.7. Principales vulnerabilidades del <i>software</i>	195
6.7.1. Desbordamiento de memoria en C/C++ (desbordamiento de búfer)	197
6.7.2. Análisis de funciones vulnerables	202
6.7.3. Vulnerabilidad de validación de entrada	204
Enlaces web de interés	206
Actividades finales.	207

7. HACKING ÉTICO Y HERRAMIENTAS DE ANÁLISIS DE RED

211

7.1. Introducción al <i>hacking</i> ético	212
7.1.1. Tipos de <i>hacking</i> ético.	213
7.1.2. Fases de un <i>hacking</i> ético	214
7.2. Introducción a las auditorías	215
7.2.1. Estándares de auditoría informática.	215
7.2.2. Tipos de auditorías	216
7.3. Auditoría de sistemas y redes.	217
7.3.1. Comprobar la seguridad de un servidor SSH	217
7.3.2. Rebex SSH Check	218
7.3.3. ssh-audit	219
7.3.4. Auditoría de redes.	221
7.3.5. Ataques de hombre en el medio (MITM).	222
7.3.6. Ataques de denegación de servicio (DOS).	224
7.3.7. Ataque DNS <i>spoofing</i>	225
7.4. Nmap como escáner de puertos	226
7.4.1. Técnicas de escaneo de puertos	228
7.4.2. Detección del sistema operativo y aplicaciones	231
7.4.3. Optimizar el escaneo de puertos.	233
7.4.4. Análisis de vulnerabilidades con nmap	233
7.5. Escáneres de seguridad <i>open source</i>	234
7.5.1. Arachni	235
7.6. Escáneres de red	239
7.6.1. Zenmap	239
7.7. Herramientas de análisis de tráfico de red	242
7.7.1. Wireshark	243
7.7.2. NetworkMiner.	245
Enlaces web de interés	248
Actividades finales.	249

8. INTRODUCCIÓN A LA INTELIGENCIA DE FUENTES ABIERTAS (OSINT)

251

8.1. Introducción a OSINT	252
8.1.1. Ciclo de vida de OSINT	252
8.1.2. OSINT frente a investigación.	253
8.1.3. Fuentes públicas OSINT	253
8.2. OSINT como disciplina de inteligencia	255
8.2.1. El proceso de inteligencia	256



8.2.2. Disciplinas de inteligencia	256
8.2.3. Incidentes e investigaciones	258
8.2.4. Métodos de recolección de información	258
8.3. <i>Hacking</i> con buscadores	260
8.3.1. Google CSE (<i>Custom Search Engine</i>)	260
8.3.2. Google Hacking Database	261
8.3.3. Google Dorks	262
8.3.4. Búsqueda avanzada en Google y Bing con Advangle	264
8.4. Motores de búsqueda alternativos	265
8.4.1. Shodan	266
8.4.2. Censys y ZMap	268
8.4.3. Binaryedge	270
8.4.4. Otros motores de búsqueda	270
8.5. Herramientas OSINT	272
8.5.1. Recopilación de información o <i>footprinting</i>	274
8.5.2. theHarvester	276
8.5.3. Escáner de puertos	277
8.5.4. Identificación de la infraestructura y de los rangos de red	278
8.6. Herramientas para obtener información sobre un dominio	280
8.6.1. Enumeración de subdominios	282
8.6.2. Obtener subdominios con Nmap	284
8.6.3. Extracción de subdominios con Sublist3r	285
8.7. Extracción de metadatos de documentos con ExifTool	286
Enlaces web de interés	288
Actividades finales.	290

9. CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

293

9.1. Introducción al centro de operaciones de seguridad (SOC)	294
9.1.1. Vectores para construir un SOC	294
9.1.2. Características y construcción de un SOC	295
9.2. Respuesta a incidentes de ciberseguridad	296
9.2.1. Preparación	297
9.2.2. Detección y análisis	297
9.2.3. Contención y recuperación	298
9.2.4. Actividades posincidente	299
9.3. Gestión de vulnerabilidades	300
9.3.1. Análisis de vulnerabilidades	300
9.3.2. Repositorios de vulnerabilidades	304
9.3.3. Explotación de vulnerabilidades	308
9.4. Herramientas SIEM de monitorización de <i>logs</i>	309
9.4.1. Introducción a los SIEM	309
9.4.2. Gestión de eventos en los SIEM	310
9.4.3. Ventajas de los SIEM	311
9.4.4. Introducción al ELK Stack	313
9.4.5. Otro <i>software</i> SIEM	319
9.5. Sistemas de detección de intrusos (IDS)	319
9.5.1. Limitaciones de los IDS	320
9.5.2. Tipos de sistemas de detección de intrusos	321
9.5.3. Snort como sistema de detección de intrusos	324
9.6. Otras herramientas que actúan como IDS	331
Enlaces web de interés	333
Actividades finales.	334

