

MARÍA ÁNGELES CABALLERO
DIEGO CILLEROS SERRANO

EL LIBRO DEL HACKER

EDICIÓN 2022

ANAYA
MULTIMEDIA

**EL LIBRO DEL
HACKER**
EDICIÓN 2022

EL LIBRO DEL HACKER

EDICIÓN 2022

**MARÍA ÁNGELES CABALLERO
DIEGO CILLEROS SERRANO**

ANAYA
MULTIMEDIA

Responsable editorial: Víctor Manuel Ruiz Calderón

Diseño de cubierta: Celia Antón Santos

Ilustraciones de cubierta, portadillas y de páginas 3, 26, 36, 147, 152, 169, 177, 403, 485, 487: © 2021 iStockphoto L.P. /Getty Images

Primera edición electrónica 2021

Todos los nombres propios de programas, sistemas operativos, equipos hardware, etc. que aparecen en este libro son marcas registradas de sus respectivas compañías u organizaciones.

Reservados todos los derechos. El contenido de esta obra está protegido por la Ley, que establece penas de prisión y/o multas, además de las correspondientes indemnizaciones por daños y perjuicios, para quienes reprodujeren, plagiaren, distribuyeren o comunicaren públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la preceptiva autorización.

© EDICIONES ANAYA MULTIMEDIA (GRUPO ANAYA, S.A.), 2022

Juan Ignacio Luca de Tena, 15. 28027 Madrid

ISBN: 978-84-415-4444-4

Edición digital sobre la 1.ª edición impresa 2021

*A Ariadna, nuestra hija, por ser nuestra inspiración,
por toda esa ternura que desprendes y tus maravillosas sonrisas.
Nos has hecho entender lo que es el amor incondicional, infinito, indescriptible.
Por toda una vida llena de alegrías que nos espera junto a ti. ¡Te queremos, bombón!*

Agradecimientos

Queremos agradecer este libro a nuestras familias y amigos que siempre nos han apoyado cuando hemos hecho este tipo de proyectos, así como expresar nuestro agradecimiento por el respaldo recibido por nuestros compañeros de trabajo, que nos han asesorado y apoyado en todo momento y sabemos que lo seguirán haciendo en un futuro.

La ciberseguridad, tanto desde un punto de vista más técnico como más conceptual, es un mundo complejo y en constante evolución, por lo que siempre tenemos que estar actualizándonos y aprendiendo nuevos conceptos, técnicas y herramientas, lo que nos lleva a pasar muchas horas de estudio y análisis. En esos momentos de retiro nunca nos falta el apoyo de nuestros seres queridos, que nos ayudan y comprenden. Por todo ello, les damos las gracias y esperamos que sigan soportando los nuevos retos que seguro llevaremos a cabo en el futuro.

Desearíamos expresar nuestra máxima gratitud a todos los lectores de este libro, ya que sin ellos esto no sería posible. Esperamos aportar conocimientos de gran utilidad e innovadores, para que el lector aprenda con cada página, al igual que nosotros lo hemos hecho durante el desarrollo de la obra.

Sería desleal por nuestra parte no acordarnos y agradecer, además, a todos los cibernautas que desarrollan y aportan su conocimiento de manera desinteresada en Internet, a todos los foros de seguridad y *hacking* en la red. Gracias también a Internet y a sus creadores por haber cambiado el mundo en el que vivimos y que nos permite intercambiar conocimientos sin importar el lugar ni el tiempo.

Para terminar, agradecer de manera muy especial a Anaya Multimedia por darnos una nueva oportunidad y por el interés y ganas que han puesto en este libro, confiando en la materia que trata. También dar las gracias al editor, Víctor Manuel Ruiz, que siempre pone todos sus medios para ayudarnos en la realización de un nuevo libro.

Por último, queríamos agradecer la inestimable aportación en el libro de Pilar Gandía Herrero, doctora en Psicología, por ayudarnos a entender cuál es la psicología del cibercriminal en un capítulo novedoso y muy didáctico.

A todos ellos muchas gracias.

Sobre los autores

María Ángeles Caballero Velasco

María Ángeles Caballero Velasco cuenta con más de 10 años de experiencia en el sector de la ciberseguridad. Actualmente es *Head of Cybersecurity* para una de las principales entidades del Banco Santander en el ámbito de CISO (Chief Information Security Officer). Es ingeniera en Informática Técnica de Gestión y licenciada en Administración y Dirección de Empresas por la Universidad Carlos III de Madrid. También ha cursado el Máster Universitario en Seguridad de las TIC por la UEM y el Máster en Design Thinking por el MIT. Posee múltiples certificaciones como CISSP, SSCP, CEH o PMP y tiene numerosas publicaciones en libros, revistas y foros, habiendo publicado 7 libros de ciberseguridad hasta la fecha. Ha participado en múltiples seminarios, conferencias y cursos, dado que le entusiasma la concienciación y la formación. Finalmente, su pasión por el comportamiento y la cognición humana le ha llevado a estar cursando actualmente el Grado de Psicología por la UNED y a certificarse como *coach profesional* con la escuela americana IPEC.



es.linkedin.com/in/angelescaballero.

Diego Cilleros Serrano

Es ingeniero superior de Telecomunicaciones por la Universidad Carlos III de Madrid y estudiante de Grado de Criminología por la Universidad Internacional de La Rioja. Su experiencia profesional ha estado siempre ligada al mundo de las redes de datos y de la ciberseguridad, trabaja actualmente como gerente *senior* de ciberseguridad en el área Cyber Risk Services de Deloitte España y es responsable de un equipo cercano a las 100 personas dedicado a las arquitecturas de seguridad y a la seguridad *cloud*. Posee diferentes certificaciones de ciberseguridad que complementan su experiencia, como Offensive Security Certified Professional (OSCP), Certified SCADA Security Architect (CSSA), CISSP, CCSP, CSX y CISA, y algunas relacionadas con AWS y Azure, entre otras. Ha participado en diferentes seminarios y cursos, y es coautor de diferentes publicaciones sobre ciberseguridad.



es.linkedin.com/in/diegocilleros.

Sobre los colaboradores directos

Pilar Gandía Herrero

Doctora en Psicología por la Universidad de Murcia, y profesora en el departamento de Psicología Básica y Metodología de esta universidad. Cuenta con 10 años de experiencia en su ámbito. Es psicóloga forense y perito en ejercicio privado. Realizó el Máster en Psicología de la Intervención Social, intensificando su formación en la psicología jurídica y forense. Además, ha sido formadora en varios cursos relacionados con esta temática, y actualmente imparte docencia en el grado de Psicología, y en los Másteres Oficiales de Abogacía y de Psicología Jurídica. Compagina el desarrollo privado de la profesión y la docencia con la investigación, siendo sus principales aportaciones al ámbito de la psicología jurídica.

Índice de contenidos

Agradecimientos	6
Sobre los autores.....	7
Sobre los colaboradores directos	8

INTRODUCCIÓN 19

Nuevas tecnologías, nuevos retos.....	19
Objetivos del libro.....	20
Organización del libro	21

1. EL MUNDO DIGITAL ES INSEGURO 25

Tiempos de incertidumbre	25
Grandes cifras.....	28
Filosofía <i>hacker</i> y argot	35
<i>White hat, sneaker</i> o hacker ético	37
<i>Black hats</i> o <i>crackers</i>	38
<i>Grey hats</i>	38
<i>Insiders</i>	38
<i>Script kiddies</i>	39
<i>Phreakers</i>	39
Conceptos y enfoques	39
Conceptos básicos de seguridad: CIA	40
Triángulo de seguridad, funcionalidad y facilidad de uso.....	40
Enfoque de perímetro de seguridad.....	41
Zero Trust.....	42
Defensa en profundidad o enfoque de seguridad por capas	43
Metodologías y estándares en ciberseguridad.....	43
NIST Cybersercurity Framework.....	43

Recursos de seguridad <i>online</i>	50
Leyes y normativas de aplicación nacional.....	52
Estrategia de Ciberseguridad Nacional	53
Ley de Protección de Infraestructuras Críticas	55
Instituciones	55

2. CIBERAMENAZAS 59

Trabajando en remoto de manera segura.....	59
<i>Threat actors</i>	60
Panorama de las ciberamenazas	61
<i>Phishing</i> e ingeniería social	63
Cómo protegernos	70
<i>Malware</i> y <i>ransomware</i>	72
SIM Swapping.....	81
Errores, entrega incorrecta y mala configuración.....	84
Supply Chain Attack	87
<i>Distributed Denial of Service</i> o denegación de servicio distribuido	92
<i>Cryptojacking</i>	96
Uso de credenciales robadas.....	100
La cadena de ataque.....	103
Pasos y etapas	104
<i>Cyber Kill Chain</i>	107
MITRE ATT&CK™	108

3. CIBERGUERRA 113

Introducción	113
Ciberguerra, ciberespionaje y ciberataques	115
Historia de la ciberguerra	115
Stuxnet, "el <i>malware</i> más inteligente jamás visto"	118
¿Quién creó Stuxnet?	119
Algo sobre su historia.....	119
Propagación de Stuxnet	121
APT & <i>Targeted Attacks</i>	122
Vías de infección	123
¿Quién crea los APT?.....	123
Ejemplo práctico de un APT y metodología de análisis.....	124
Detección del APT.....	125
Análisis del correo electrónico original	126
Análisis del adjunto malicioso	132
Análisis del código fuente del fichero	132
Reproducción del ataque	136

4. HACKER MINDSET 141

Término <i>hacker</i>	141
Introducción	141
Desde la psicología	142
¿Hablamos de estereotipos o de perfiles criminales?	142
El cibercriminal como agente del delito	145
Refuerzo emocional	148
¿Quiénes son los más vulnerables?	152
Influencia y persuasión	153
Actores de amenazas	159
Motivaciones y sofisticación	160
Entendiendo las motivaciones	162
Ciberterrorismo	165
Crimen organizado	166
Hacktivistas	168
Lobos solitarios	171
<i>Insiders</i>	174

5. ARQUITECTURAS DE RED Y DATOS: DEFENSA Y OFENSIVA 181

Introducción	181
Conceptos de red y comunicaciones	182
Modelo OSI vs. Modelo TCP/IP	182
IPv4	185
IPv6	191
TCP	195
Consideraciones de seguridad sobre protocolos	200
Hardware de red	202
Arquitecturas de red	204
La seguridad en la red de datos	205
<i>Firewalls</i>	206
VPN	208
DLP	209
Arquitecturas de seguridad	210
Otros elementos de seguridad	212
Zero Trust	215
Protección de infraestructuras en la nube	216
Próximos enfoques: ZTNA y SASE	217
Ofensiva en la red	220
Ataques a nivel de red	220
Wireless: Wi-Fi	223
VoIP	248

6. MUNDO INDUSTRIAL E IOT 265

Industria 4.0.....	265
Conceptos y arquitectura de SCADA.....	267
Seguridad en entornos SCADA.....	271
Desmitificando los ataques sobre SCADA	274
Breve introducción a IoT	281
El reto de la seguridad IoT	282

7. HACKING WEB Y SEGURIDAD EN MICROSERVICIOS 285

Introducción	285
OWASP Top 10.....	286
WebGoat	288
Metodología.....	289
Proxy web	290
Mapeado web.....	291
Análisis automático de vulnerabilidades web	293
Inyección	299
Inyección de comandos	299
SQL Injection	302
Cross-Site Scripting (XSS).....	311
XSS almacenado o persistente	312
XSS reflejado	312
XSS basado en el DOM	313
Servidor vs. Cliente.....	313
Puesta en práctica	313
Inclusión de ficheros.....	317
LFI	318
RFI.....	321
Otros controles.....	323
Sistemas de gestión de contenidos	324
Análisis de Wordpress	325
Microservicios y contenedores.....	332
Tecnología de contenedores	335
Docker	336
Seguridad en contenedores	343
Cloud Workload Protection	349

8. CLOUD 351

Introducción	351
Los conceptos a conocer.....	354
Nube pública.....	362
Riesgos	363

Amazon Web Services (AWS)	365
Microsoft Azure	375
Google Cloud Platform (GCP)	382
Estrategia de seguridad	385
Buenas prácticas de seguridad	386
Framework de controles y monitorización del cumplimiento	389
Protección de los datos en entornos SaaS	393

9. IDENTIDAD DIGITAL Y BIOMETRÍA 397

Futuro de la identidad digital	397
Introducción	398
Empoderando al individuo	399
¿Qué tecnologías determinarán el camino de nuestra identidad digital?	400
Identidad digital y Blockchain	401
Self Sovereign Identity	402
Aproximaciones privadas y gubernamentales	404
ESSIF	404
Alastria	406
Registro CI@ve	406
Registros nacionales de identidades digitales	407
Identidad digital	408
Pero ¿qué es la identidad? ¿Y la identidad digital?	408
Ciclo de la identidad digital	410
Onboarding digital	412
Identity as a Service (IDaaS)	415
Proveedores de identidad	417
Autenticación	418
Métodos de autenticación	419
Ataques y técnicas a la identidad digital	427
Credencial Access TTP	427
Ataque a Kerberos: Golden Ticket	431
Biometría	438
Definición y origen	438
Modelos biométricos	439
Biometría comportamental o conductual	443

10. CRIPTOGRAFÍA Y BLOCKCHAIN 447

Introducción	447
Definición y tipos de sistemas criptográficos	448
Criptografía de clave simétrica	448
Sistemas clásicos	449
Sistemas modernos	450

Criptografía de clave pública	455
RSA	456
ElGamal	457
Algoritmos de Hash.....	458
MD5	459
SHA-1.....	460
SHA-2.....	460
SHA-3.....	461
Herramientas de análisis.....	461
La firma electrónica	463
Certificados digitales.....	464
Ámbitos de aplicación	470
Algunas aplicaciones y protocolos.....	472
SSL/TLS.....	472
IPSec	475
SSH	476
Firma electrónica de documentos.....	476
Beneficios de la firma electrónica.....	476
Firma electrónica vs. firma digital.....	478
Tipos de firma electrónica vs. legislación	478
Ataques y programas de análisis.....	479
Fuerza bruta distribuida.....	479
Tablas Rainbow	480
Cryptool.....	480
Aircrack-ng.....	480
John the Ripper	480
Cain & Abel	481
mitmproxy.....	482
sslstrip.....	482
Blockchain	482
Historia de Blockchain: Bitcoin.....	484
Ataques a la red de Bitcoin	485
<i>Smart contracts</i>	486
Ethereum	487
Características de las redes Blockchain	488
Algoritmos de consenso	489
Inmutabilidad.....	497
Como conclusión	497
Proyectos y redes de Blockchain.....	498
Hyperledger.....	498
Quorum	499
Ripple.....	500
Redes públicas y privadas	500
Blockchain públicas	500

Blockchain privadas	501
Blockchain híbridas	504
Trilema de la escalabilidad	505
Descentralización.....	506
Seguridad	506
Escalabilidad.....	507
Como conclusión	509
Retos de seguridad y amenazas de Blockchain	509
Amenazas	509
Ataques a la tecnología	512
Blockchain en la <i>dark web</i>	513
¿Qué es la <i>dark web</i> ?	513
¿Cómo puede apoyar Blockchain a la <i>dark web</i> ?	515
Ámbitos de aplicación.....	517
Un caso de uso apasionado que deberías conocer: diamantes de sangre.....	519

11. METODOLOGÍA DE PENTESTING

521

Introducción	521
Metodologías	522
OWASP.....	523
OSSTMM	525
NIST SP800-115.....	525
Fases generales de un test de intrusión.....	526
<i>Information Gathering</i> : información pública.....	527
Reconocimiento del DNS	528
Google Hacking.....	533
Otras herramientas útiles para la búsqueda de información pública.....	540
<i>Information Gathering</i> : consulta activa.....	542
Enumeración de activos mediante DNS.....	543
Uso de ICMP.....	544
Escaneo de objetivos.....	545
Técnicas de enumeración	552
Análisis de vulnerabilidades	557
Clasificación y fuentes	557
Fabricantes	559
Herramientas	561
Trabajar con <i>exploits</i>	563
Metasploit.....	564
Componentes de Metasploit.....	565
<i>Exploits</i>	570
Uso de Metasploit	571
Explotación manual	574
EternalBlue	575

Escalado de privilegios.....	582
Vulnerabilidades en el sistema operativo	583
Escalado con Meterpreter	587
Ataques a credenciales	590
Credenciales comprometidas.....	591
Ataques.....	592
Gestión de las credenciales en Linux	595
Robando credenciales en Linux.....	599
Gestión de credenciales en Windows	602
Robando credenciales en Windows	608
Credenciales en equipos de red.....	614
Captura de tráfico en la red	614
Wireshark	615
Finalizando una intrusión.....	619
Eliminar las evidencias de un ataque.....	619
Trabajo en equipo	620
Diferencias y definiciones	621
Misiones basadas en inteligencia de amenazas	624

12. EXPLOITING 627

Introducción	627
Pila	628
Registros	628
Instrucciones de ensamblador	629
Buffer overflow	630
Fuzzing.....	633
Controlar el registro EIP	636
Bad characters	641
Búsqueda de direcciones de retorno y ejecución de código.....	642
Backdoors en aplicaciones portables.....	646
Demostración de inserción de código manual.....	647
Uso de herramientas automáticas	654

13. DATA EXFILTRATION 657

Introducción	657
Casuísticas	658
Estadísticas y casos actuales.....	660
Clasificación de la información.....	662
Técnicas y tácticas de ataque	664
Fugas en herramientas colaborativas.....	670
Controles de protección del dato	671
Protección de datos almacenados	672
Protección de datos en movimiento	672

14. ANÁLISIS FORENSE

675

Introducción	675
Ciencia e informática forense	675
Principios de la informática forense	677
Principio de transferencia de Locard	677
Borrado parcial de información en los dispositivos de almacenamiento electrónico ...	678
Memoria virtual y archivos temporales	679
Guías y definiciones	680
La evidencia digital	681
Ciclo de vida para la administración de la evidencia digital	681
Tipos de análisis forense y dispositivos	684
Discos duros	685
Motivos de un análisis forense	686
Uso particular o negocio	686
Legal y cibercrimen	687
Etapas de una investigación forense	688
Estudio	688
Adquisición	688
Análisis	689
Presentación	689
CSIRT	690
Incidente	690
Análisis forense en un CSIRT	691
CSIRT españoles	691
Herramientas forenses	692
Clasificación de herramientas	693
Herramientas de análisis	711
Análisis sencillo sobre Windows	714
Motivo del análisis	715
Información del sistema operativo	715
Información de red	720
Información de tareas, aplicaciones, componentes, servicios y otros	720
Información sobre <i>malware</i>	726
Información acerca de la actividad del usuario	728
Información acerca de los ficheros temporales	729
Información acerca del historial de navegación	730
Retos del forense en entornos <i>cloud</i>	735

ÍNDICE ALFABÉTICO

736



Introducción

Nuevas tecnologías, nuevos retos

Vivimos rodeados de tecnología, vayamos donde vayamos y hagamos lo que hagamos, siempre nos apoyamos en ella. Cada vez más, a veces sin darnos cuenta, utilizamos nuestros *smartphones*, o incluso *wearables*, para realizar todo tipo de transacciones y procesos de nuestro día a día. Volcamos todo tipo de información de nuestra vida, nuestras aficiones y nuestros gustos, y nos comunicamos con todo tipo de personas, a través de las redes sociales. Buscamos todo tipo de información y compramos muchos productos a través de la gran cantidad de portales donde se vende casi de todo sin tener que movernos de nuestra casa. Toda esta información que movemos desde nuestro teléfono de última generación, *tablet* u ordenador personal podría estar comprometida y sería accesible a un intruso malintencionado si no tomamos las medidas oportunas.

No es raro leer en los medios de comunicación noticias que tratan de identidades suplantadas y datos robados a través de Internet. Los usuarios debemos concienciarnos (y concienciar) de lo vulnerables que podemos llegar a ser cuando no controlamos ni conocemos la manera en la que los datos se están moviendo y almacenando en la red, acrecentándose este desconcierto con la famosa nube o *cloud*.

Nunca le daría su número de cuenta bancaria o su tarjeta de crédito a otra persona, pero ¿qué pasa si las escribo en una página web donde voy a realizar una compra? Muchas veces confiamos en portales de venta de productos, simplemente porque vemos logotipos de empresas certificadoras o de verificación de calidad, pero ¿podrían estar engañándonos? ¿Podría no tratarse de esa empresa que dice ser?

Y esto no es un problema que tengamos únicamente en el ámbito personal; en el ámbito profesional, donde el objetivo de los cibercriminales es mucho mayor y el impacto puede ser terrible, las personas seguimos siendo el eslabón más débil de la cadena. No importa si nuestra empresa se gasta millones de euros en adquirir tecnología avanzada de protección del perímetro, protección del puesto de usuario, medidas *antiransomware* y tecnologías disruptivas (*web isolation*, *cloud workload protection*, etc.), los usuarios de los recursos tecnológicos de nuestra compañía debemos ser cautelosos frente a todas las amenazas que se nos presentan, ya que vamos a ser los objetivos de los atacantes para conseguir una vía de entrada a la información y sistemas de una organización.

El ciberespacio es un mundo ideal donde podemos hacer casi cualquier cosa sin salir de nuestra casa, pero es tanta y tan variada la información que movemos a través de la red, que es lógico pensar que será muy cotizada por todo tipo de usuarios malintencionados. Por ello, debemos conocer muy bien cómo funcionan los distintos portales de Internet y con qué medidas de protección contamos para poder hacer uso de la tecnología, sin que ello nos provoque un problema de privacidad o seguridad de nuestra información.

A través de este libro le presentaremos la ciberseguridad y las nuevas tecnologías, poniendo al descubierto sus debilidades y enseñándole a protegerse de ellas. Veremos cómo hacer los sistemas más seguros y que sea capaz de utilizar todo tipo de herramientas y servicios en la red, sabiendo que la privacidad de su información y sus datos se encuentran totalmente seguros.

Objetivos del libro

Nos encontramos ante un libro técnico que, de manera clara y concisa, nos enumera las diferentes técnicas y herramientas de seguridad y ciberataques disponibles sobre las más actuales tecnologías.

Creemos fundamental que el usuario se sienta confortable cuando navegue por Internet y que domine los conceptos básicos de ciberseguridad y privacidad de la información. Por ello, lo que pretendemos es que, tras la lectura de este libro, tenga claro las amenazas y vulnerabilidades de los sistemas de información y pueda tomar las medidas oportunas para protegerse de ellas.

Podemos decir que con estas páginas despertaremos un deseo por conocer y aprender mucho más de los sistemas, así como las ganas de estar al día y seguir formándose en el mundo de la ciberseguridad, pues este entorno es como un ser vivo, evoluciona día a día con nuevas herramientas y servicios.

- PCI-DSS, 209, 294, 559, 562
- Perfil criminal, 141-176
- Phreakers*, 37, 39
- Pivotar, 215, 230
- PKI, 234, 425, 465, 469, 471
- Port forwarding*, 190
- Pretexting*, 65
- Principio de transferencia de Locard, 677
- Principios de seguridad, 40
- ProLock, 77
- Protocolo
 - ARP, 193, 200, 547, 615
 - BGP, 201
 - de *tunneling*, 106
 - DHCP, 186, 201, 258
 - DNS, 42, 94, 528, 531, 543
 - DTLS, 255
 - FTP, 199, 592, 597, 615, 632, 636, 641, 646, 697, 709
 - HTTP, 92, 95, 199, 249, 254, 276, 290, 297, 312, 320, 482, 540, 550, 633, 667
 - HTTPs, 200, 290, 420, 472, 482, 667
 - ICMP, 92, 189, 193, 207, 544, 547, 549
 - IMAP, 200, 555
 - LDAP, 200, 251, 286, 293, 339, 416, 552, 556
 - NDP, 193, 195
 - NetBIOS, 200, 606
 - NTP, 200, 597
 - PDU, 195, 270
 - POP3, 199, 555
 - RPC, 199, 550, 573, 597
 - RSH, 476
 - SLAAC, 191, 194-195
 - SMB, 200, 428, 571, 576
 - SMTP, 130, 555, 633, 666
 - SNMP, 200, 206, 552-553
 - SSH, 36, 199, 251, 476, 548, 550, 619, 673, 677
 - STP, 201
 - Syslog, 206, 620
 - TCP/IP, 92, 182, 189, 269, 271, 472, 476, 556
 - Telnet, 199, 476, 553, 555, 592, 615
 - TFTP, 199, 258
 - UDP, 92, 124, 185, 198, 249, 252, 508, 544, 549, 707
- Protocolo ICS, 269, 270, 276-280
- Protocolo Wireless
 - WEP, 228, 239, 453, 480
 - WPA, 228, 230, 240
 - WPA2, 223, 235, 240, 245, 247
- Proxy*, *Proxies*, 106, 289, 292, 528, 540, 581, 689
- PSK, 229, 233, 240, 242, 244

R

- Radio Frequency Interference*, 183, 668
- RADIUS, 226, 229, 233, 240, 251
- RADIUS Autenticación, 233
- Ransomware-as-a-Service* (RaaS), 73

- Rapid7, 311, 564
- Reconocimiento activo, 91, 105
- Reconocimiento pasivo, 105
- Red
 - DMZ, 273
 - social
 - Facebook, 64, 117, 170, 668
 - Instagram, 64, 82, 662
 - LinkedIn, 82
 - Pinterest, 177
 - TikTok, 82, 662
 - Twitter, 70, 83, 118
 - YouTube, 90, 348, 509
 - Team, 621, 624, 625
 - TOR, 106, 214, 528
 - VoIP, 248, 250, 257
 - Wireless, 615
- Redes
 - LAN, 119, 190, 202-204, 206
 - MAN, 204
 - SD-WAN, 220
 - VLAN, 202, 204, 256-258
 - WAN, 204, 220, 378
 - Wi-Fi/WiFi, 74, 105, 223-227, 230, 232, 234-236, 240-241, 246-248, 668
- Registro DNS, 531
- Remote File Inclusion*, 183, 318-319, 321-322
- Repetidor, 203
- Repositorio LDAP, 200, 251, 416, 552, 556
- Revocación de certificados, 469
- Roguesoftware*, 72, 76
- RootedCON, 348
- Rootkits*, 72, 74, 106, 119, 294, 384, 699
- Router, 188, 190, 194-195, 201, 204, 234-235
- Ryuk, 73, 77, 90-91

S

- S/MIME, 40, 255
- SAM, 429, 602-603, 606-608, 611-612
- SAML, 428
- Sandbox*, 79, 132, 136
- SANS Institute, 51, 559, 693-694
- SASE (*Secure Access Service Edge*), 28, 42, 217, 219-220
- SCADA, 22, 67, 118-119, 121, 266-269, 271-277, 280-281
- SCAP, 558
- SCAPY/Python, 201, 263
- Script Kiddie*, 37, 39, 61, 78, 86, 100, 171
- SDescriptions, 255
- Security Association, 475
- Seguridad perimetral, 42, 273, 689
- SEI, 559
- Self Sovereign Identity* (SSI), 401-402, 404
- Servicios web
 - GET, 95, 214, 292, 318
 - POST, 214, 292, 310, 319, 667

- REST, 294, 430
- SOAP, 324
- WSDL, 324
- Servidor Web Apache, 322, 528
- Session Hijacking* (Robos de sesión), 201
- Sexting*, 76
- Sharepoint*, 670
- Shell*, 310, 318, 322, 328-330, 545, 567, 583-584, 590
- Shodan, 52, 275, 542, 554
- SIEM, 125, 137, 213, 391, 444
- Single Sign-On* (SSO), 415-416, 609
- Sistema de autenticación abierto, 227, 554
- Sistema operativo móvil
 - Android, 256-257, 510, 704, 723-724
 - iOS, 256, 724
- Skype, 28, 250
- Spam*, 63, 72, 77
- Spanning Tree Protocol*, 201
- Spoofing*, 131, 184
- Spotify, 662
- Spyware*, 75
- STAR (*Security Trust Assurance and Risk*), 201, 387-388
- Suplantación de identidad, 59, 66, 82, 84, 168, 220, 445
- Switch*, 203-204
- Syskey, 205, 606-607

T

- Tablas Rainbow, 421, 480, 594
- Tácticas, técnicas y procedimientos (TTP), 164, 167, 170, 172, 177, 427, 623-624
- Tailgating*, 66
- Targetted Attack*, 122
- Telefonía móvil 3G, 668
- Telegram, 149
- Temporal Key Integrity Protocol* (TKIP), 226, 228, 230
- TERENA, 692
- Test de intrusión, 22, 37, 87, 521-522, 526, 622
- Thawte*, 466
- Threat actor*
 - Cibercriminales, 20, 60, 89, 108, 142, 148-149
 - Grupos terroristas, 61
 - Hacktivistas, 61, 78, 92, 124, 162, 168
 - Insider*, 38-39, 61, 162, 174, 176
 - Lobos solitarios, 61, 69, 78, 162, 171
 - Mafias organizadas, 38, 60, 69, 78, 82, 89, 98, 100, 161
 - Naciones, 61, 78, 162
 - Thrill seekers*, 61
- Threat landscape*, 62
- Three-Way Handshake*, 196-197, 617
- Tiger team*, 37
- Token OTP*, 421-423
- TPV, 115
- Trend Micro, 129, 726
- Triángulo
 - Confianza, 403
 - Facilidad de uso, 40-41

- Funcionalidad, 40-41
- Seguridad, 40-41
- Trickbot*, 73, 77
- Troyano, 67, 72-74, 76-78, 114-115, 423, 662
- Trusted Introducer*, 692
- Trusted Platform Module*, 424

U

- Ubuntu, 336, 560-561
- UFS Sun Solaris, 561, 695, 701
- Universidad Carnegie Mellon, 50, 559, 690
- USB Condoms, 68
- US-CERT, 50, 559
- Usuario
 - administrator, 181, 300, 331, 433, 589
 - root, 74, 106, 335-336, 348

V

- Vector de inicialización (IV), 228, 238
- Verisign, 466
- VLAN Hopping*, 257
- VLAN Trunking Protocol*, 202
- VocalTec Communications, 248
- VOIP protocolos, 248-249, 251
- VPN, 208-209, 216, 378

W

- WAF, 96, 214, 287, 294, 373
- WannaCry, 85, 113, 162-163, 165, 575
- We Are Social, 28, 255
- Web of trust, 466
- WebGoat, 288-289, 300, 302-303, 310, 313-314, 316
- WECA, 223
- WhatsApp, 82
- Wi-Fi Protected Setup* (WPS), 240-244
- WikiLeaks, 117, 170
- Willis Ware, 521
- WinPCap, 608
- WNIC, 230
- WPScan, 326-327

X

- X.509, 255, 426, 467-469
- XSS, 106, 287, 311-312, 316-317, 524

Z

- Zero day*, 42, 84-86, 105, 114, 119, 217
- Zero Trust, 42, 215
- Zero-Trust Network Access* (ZTNA), 11, 215, 217-220