EN CONSTRUCCIÓN. La ciberseguridad insegura: sacando los colores a la sociedad digital

Autor: Jorge Dávila
Prólogo: Luis Jiménez
Editorial: Ediciones CODA
Año: 2021 – 792 páginas
www.revistasic.com

El profesor y director del Laboratorio de Criptografía de la Facultad de Informática de la UPM, **Jorge Dávila**, es uno de los grandes referentes académicos en ciberseguridad y nuevas tecnologías. Desde el año 2000, su sección 'en Construcción', en Revista SIC, se ha erigido como una de las atalayas del pensamiento digital sobre los riesgos y parabienes de las nuevas tendencias que presumen con cambiar el mundo, ya sea la inteligencia artificial, la identidad, la analítica de datos masiva, la automatización y, por supuesto, el cómo aportar ciberprotección a un mundo cada vez más hiperconectado. Ahora, Ediciones Coda, editora de la Revista, ha querido celebrar sus 30 años de vida agrupando sus 101 artículos durante más de 20 años en una recopilación que, por su profundidad, didactismo y, también, reflexión, son de obligada lectura para los que quieren saber qué hay detrás de toda esa tecnología que usamos cada día y cómo, empezando por las personas, podemos ayudar a que sea más segura. La obra, prologada por el Subdirector del CCN, del CNI, **Luis Jiménez**, además del editor de Revista SIC, **Luis Fernández**, y su director, **José de la Peña**, no dejará indiferente a nadie siendo de 'lectura obligatoria' para los que buscan desasnarse. **Revista SIC** inicia 2021 con la celebración de sus 30 años de vida regalando esta obra recopilatoria, que se puede solicitar en PDF o ePUB en www.revistasic.com

DESINFORMACIÓN Y GUERRA POLÍTICA

Autor: Thomas Rid
Editorial: Critica
Año: 2021 – 552 páginas
ISBN: 978-84-91-992776
www.planetadelibros.com

Apasionante obra sobre la información y desinformación como estrategia durante todo el siglo XX y, también, el XXI. Rid, reconocido experto sobre tecnología y espionaje, fue uno de los primeros en alertar de la posible injerencia rusa en las elecciones estadounidenses, en 2016.

En este libro, desgrana y lleva al lector a la 'trastienda' de los servicios secretos y de cómo realizan muchas de sus operaciones en el ciberespacio hackeando, filtrando información y falsificando datos para minar "nuestra confianza en la información y debilitar la base misma de la democracia". La obra, escrita de forma amena y con abundante información y bibliografía sobre la materia, ofrece un asombroso viaje por "un siglo de guerra psicológica secreta" con algunas de las operaciones más significativas de la historia a través de las que cómo los espías comenzaron a explotar la cultura emergente de Internet mucho antes del caso WikiLeaks.

En cierto modo, como explica su autor, el libro "conduce, como si de una visita guiada se tratara, por lo más profundo de un vasto salón de espejos, antiguos y nuevos, apuntando a un futuro de polarización diseñada, pero también nos ofrece las herramientas para superar este engaño". Sin duda, una obra que se convertirá en breve en lectura obligada para los que quieren saber de la desinformación, sus técnicas y qué impacto tiene y tendrá en la sociedad.

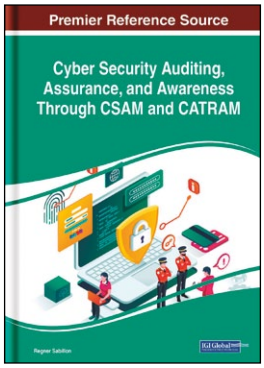
BUG BOUNTY: De profesión cazarrecompensas

Autor: Pablo García
Editorial: 0xword
Año: 2021 – 258 páginas
ISBN: 978-84-09-25909-0
0xword.com

Pablo García está especializado en Auditoría de Cuentas, pero su pasión en su tiempo libre es, desde hace años, reportar vulnerabilidades. De hecho, forma parte del 'Salón de la Fama' de compañías como Netflix, Xiaomi o Pinterest, entre otras. Precisamente su experiencia –y la escasa bibliografía en la materia- le ha llevado a publicar esta obra sobre los programas de recompensas (conocidos como *Bug Bounties*) que cada vez más empresas y organismos incorporan a sus sistemas de seguridad para que investigadores en la materia (especialmente, *hackers*) puedan buscar y reportar vulnerabilidades. Un negocio al alza: Sirva como ejemplo que, sólo entre 2019 y 2020, siete investigadores obtuvieron un total de más de 950.000 euros de recompensa, a través de la plataforma HackerOne.

Para ofrecer una visión realista, con sus claros y sombras, y facilitar a los menos expertos en este campo un 'paso a paso' sobre cómo comenzar, García aborda los aspectos básicos de estos programas, como pueden ser su estructura, las principales herramientas, ciertas metodologías o las vulnerabilidades más comunes. Todo ello, desde un punto de vista práctico analizando reportes públicos realizados por *hackers* de la comunidad. Una obra que, sin duda, por ser de las primeras en castellano, aspira a ser una de las referencias.

CYBER SECURITY AUDITING, ASSURANCE, AND AWARENESS THROUGH CSAM AND CATRAM (Auditoría, garantía y concienciación de ciberseguridad a través de CSAM y CATRAM)

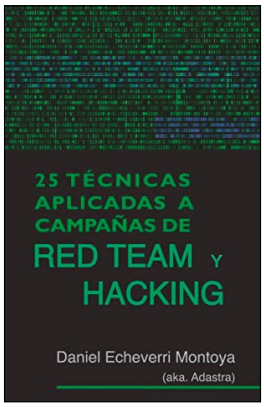


Autor: Regner Sabillón
Editorial: Igi Glogal
Año: 2021 – 260 páginas
ISBN: 9781799841623
www.igi-global.com

Regner Sabillón, profesor en la Escuela de Computación de la canadiense Athabasca University y doctorando de la UOC, explora en este libro, reconocido como mejor recomendación para 2021 sobre ciberseguridad según la web BookAuthority, los aspectos prácticos de reevaluar las medidas de ciberseguridad actuales dentro de las organizaciones y los gobiernos internacionales y mejorarlas utilizando modelos de capacitación en auditoría y concienciación, específicamente el Modelo de Auditoría de Ciberseguridad (CSAM) y el Modelo de Capacitación en Concienciación sobre Ciberseguridad (CATRAM).

Además, presenta estudios de múltiples casos sobre el desarrollo y la validación de estos modelos y marcos, y analiza su implementación y capacidad para sostener y auditar las estrategias nacionales de ciberseguridad. Con cobertura sobre un amplio abanico de temas como análisis forense, evidencia digital y gestión de incidentes, este libro está pensado, especialmente, para investigadores, desarrolladores, legisladores, funcionarios gubernamentales, estrategas, profesionales de la seguridad, educadores, analistas de seguridad y auditores, entre otros.

25 TÉCNICAS APLICADAS A CAMPAÑAS DE RED TEAM Y HACKING



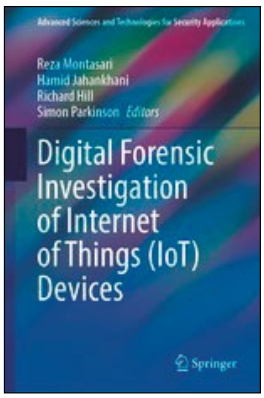
Autor: Daniel Echeverri Montoya
Editorial: Independiente
Año: 2021 – 318 páginas
ISBN: 979-8706390662
www.amazon.es

Daniel Echeverri, conocido en el mundo técnico de la ciberseguridad por 'Adastra' y autor del blog 'The Hacker Way', es un profesional con gran experiencia en Red Team en España. Este libro, de carácter técnico, nace de su afán por dar a conocer los aspectos más desconocidos del día a día de su trabajo como consultor en ciberprotección. Así, en él, explora cada una de las etapas involucradas en una campaña de Red Team. Además, ofrece una completa visión de los procedimientos aplicados para luchar contra el cibercrimen en casos reales y, sobre todo, los detalles más relevantes que tienen en cuenta los equipos profesionales de pruebas con intrusiones de seguridad, tanto sus métodos, como procedimientos y mejores herramientas.

La obra está dividida en dos apartados para ofrecer una mejor comprensión de los aspectos más técnicos. Por un lado, concentra una parte teórica con los conceptos básicos que hay que tener y, por otro, una explicación detallada de las tácticas aplicadas por atacantes y ciberdelincuentes para perpetrar ataques contra empresas y organizaciones de cualquier tipo. El libro también tiene un componente altruista: el dinero recaudado con su venta irá destinado de forma íntegra a Unicef.

DIGITAL FORENSIC INVESTIGATION OF INTERNET OF THINGS (IoT) DEVICES

(Investigación forense digital de dispositivos de internet de las cosas)

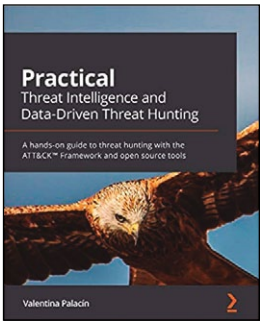


Autores: Montasari R., Jahankhani H., Hill R., Parkinson S.
Editorial: Springer
Año: 2021 – 285 páginas
ISBN: 978-3-030-60424-0
www.springer.com

La creciente popularidad de los dispositivos de IoT para actividades delictivas denota que hay disciplina y una industria en torno a la ciencia forense en esta área. A medida que la tecnología se vuelve más barata y más fácil de implementar en un mayor número de objetos cotidianos discretos, el alcance para la creación automatizada de huellas digitales personalizadas aumenta con lo que supone dejando un "rastro de datos que pueden usarse para triangular e identificar a las personas y sus acciones. Como tal, el interés y la evolución de los vehículos autónomos", destacan sus impulsores.

Para ayudar en la lucha contra el cibercrimen para los profesionales que quieran especializarse en análisis forense de IoT, tanto como parte de los cuerpos de seguridad o como miembros de los equipos de detección y respuesta a incidentes, este libro proporciona una referencia valiosa para contar con amplios conocimientos sobre la materia. De hecho, cada capítulo está escrito por un experto, de referencia internacional, con amplia experiencia en la aplicación de la ley, la industria y el mundo académico.

PRACTICAL THREAT INTELLIGENCE AND DATA-DRIVEN THREAT HUNTING: A hands-on guide to threat hunting with the ATT&CK framework and open source tools

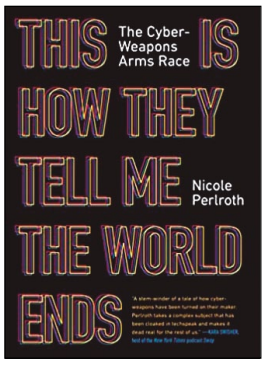


(Inteligencia práctica sobre amenazas basada en datos con el marco ATT&CK y herramientas de código abierto)

Autora: Valentina Palacín
Editorial: Publicación independiente
Año: 2021 – 398 páginas
ISBN: 978-1838556372
www.amazon.com

Valentina Palacín es una analista de inteligencia de amenazas (CTI), especializada en APTs, utilizando el marco Mitre ATT&CK, y fundadora de la comunidad BlueSpaceSec. En este manual, con un enfoque práctico, ofrece información detallada de métodos, herramientas y cómo trabaja aplicando la inteligencia a la búsqueda de amenazas (TH) basada en datos, con abundantes consejos y técnicas de expertos que participan en él. Por eso, esta obra no es una mera introducción para los que carecen de conocimiento en CTI, ni el mundo del TH, sino que se presenta como una guía para aquellos los que, con un conocimiento más avanzado de otros campos de la seguridad cibernética, buscan mejorar los suyos en este ámbito. Así pues, ofrece un paso a paso que parte sobre cómo comenzar a explorar en busca de amenazas cibernéticas para ofrecer conocimientos avanzados de cómo detectarlas y prevenirlas a través de herramientas de código abierto. Incluye ejemplos prácticos y una amplia explicación de cómo usar el marco de trabajo Mitre ATT&CK para "conseguir las habilidades necesarias".

THIS IS HOW THEY TELL ME THE WORLD ENDS: THE CYBERWEAPONS ARMS RACE



(Así me dicen que acaba el mundo: La carrera armamentista de las ciberarmas)

Autora: Nicole Perlroth
Editorial: Bloomsbury Publishing
Año: 2021 – 528 páginas
ISBN: 978-1526629852
www.bloomsbury.com/uk

La especialista en ciberseguridad del New York Times, **Nicole Perlroth**, profundiza en esta obra en los aspectos menos contados "del mercado de armas cibernéticas, el mercado más secreto, invisible y respaldado por el gobierno en la tierra, y un primer vistazo aterrador a un nuevo tipo de guerra global". Un mundo que la autora plasma en una trepidante novela llena de "espías, *hackers*, traficantes de armas y algunos héroes anónimos". El *thriller* está documentado en los años de informes y cientos de entrevistas que su autora ha realizado para el rotativo estadounidense desvelando con asombrosa nitidez la amenaza cibernética global que se cierne sobre el mundo. Se trata, en definitiva, de una forma de sacudir de su letargo a los que aún no son conscientes de los riesgos que acarrea el mundo digital a través, en muchos casos, de los propios estados. Y es que pone como ejemplo el 'arsenal' de fallos 'de día cero' que países como EE.UU. han acumulado pagando por ellos millones de dólares y que, en ocasiones, han sido robados por "naciones hostiles y mercenarios".