Fecha de Realización:	07/04/2021
Programa:	Especialización en seguridad informática
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes
Título:	HERRAMIENTAS DE RECOLECCIÓN DE INFORMACIÓN DE FUENTES PÚBLICAS, USADAS PARA PREVENIR ATAQUES DE INGENIERÍA SOCIAL EN PERSONAS Y ORGANIZACIONES EN EL CONTEXTO COLOMBIANO
Autor(es):	Alvarado Murcia John Jairo
Palabras Claves:	Open Source Intellingence, Ingeniería social, Cyberdelincuentes, Redes sociales, Ataque, Seguridad
Descripción:	En este documento encontrará información importante referente a la ciberseguridad en temas como la ingeniería social, las diferentes herramientas que son usadas para la recolección de información y la forma en que los atacantes pueden hacer uso de los datos que hacen públicos en internet, también podrán visualizar el aumento de los ataques no solo a nivel Latinoamérica sino a nivel Colombia. Se espera que esta monografía sirva de soporte, sensibilización y concientización a usuarios y empresas colombianas frente al uso y manejo de la información que es expuesta en internet, aclarando el panorama de como los atacantes usan la información pública para buscar brechas de seguridad y perfilar los ataques a un objetivo en común, pero la intensión no solo es mostrar lo que los atacantes pueden hacer sino en que también las empresas lo puedan hacer con sus equipos de ingenieros de seguridad buscando las brechas, minimizarlas o eliminarlas, el uso de las herramientas OSINT permite encontrar toda la información que se encuentre pública y endurecer o fortalecer el perímetro a través de políticas de seguridad. Adicionalmente la sensibilización y la concientización del manejo de los datos a las personas se debe hacer constantemente entendiendo que el eslabón más débil de la cadena es el usuario y de aquí dependen todas las acciones y políticas que se establecen en las organizaciones para la mitigación de incidentes o riesgos a que se puedan estar expuestas.

ALIPRANDI, C., De Luca, A. E., Di Pietro, G., Raffaelli, M., Gazzè, D., La Polla, M. N., Tesconi, M. (2014). CAPER: Crawling and analysing Facebook for intelligence purposes. 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014), 665-669. Disponible en: https://doi.org/10.1109/ASONAM.2014.6921656

BANCO INTERAMERICANO DE DESARROLLO. (2020). Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe (2020.a ed.). Disponible en: https://doi.org/10.18235/0002513

Best, C. (2012). OSINT, the Internet and Privacy. 2012 European Intelligence and Security Informatics Conference, 4-4. Disponible en: https://doi.org/10.1109/EISIC.2012.71

Butler, B., Wardman, B., & Pratt, N. (2016). REAPER: An automated, scalable solution for mass credential harvesting and OSINT. 2016 APWG Symposium on Electronic Crime Research (eCrime), 1-10. Disponible en: https://doi.org/10.1109/ECRIME.2016.7487944

Carvajal, M. (12. 2018.). Estudio de metodologías de ingeniería social. 56. CIBERSEGURIDAD: RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO. Castellano. 28 de noviembre de 2020, Disponible en: https://publicaciones.defensa.gob.es/ciberseguridad-retos-y-amenazas-a-la-seguridad-nacional-en-el-ciberespacio.html

CENTRO CIBERNÉTICO POLICIAL DE COLOMBIA. Balance_cibercrimen_2020_-_semana_45.pdf. [Consulta: 20 de febrero 2020], Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA. LEY 1928 DEL 24 DE JULIO DE 2018.pdf. [Consulta: 29 de noviembre de 2020] Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

Contenido del documento:	La presente monografía contiene cuatro objetivos dentro de los cuales se desarrolla la explicación de las herramientas OSINT usadas para prevenir ataques de ingeniería social en personas y organizaciones en el contexto colombiano. Objetivo 1: Seleccionar a partir de conceptos básicos de ingeniería social, ataques que se realizan a través del uso de herramientas de

	inteligencia de fuentes públicas. Objetivo 2: Compilar las diferentes herramientas usadas para la recolección de información de fuentes públicas. Objetivo 3: Identificar el tipo de información obtenida de fuentes públicas que puede ser usada por un atacante. Objetivo 4: Elaborar un documento guía de referente informativo para las empresas colombianas que permita ayudar a prevenir la exposición de información sensible en fuentes públicas.
Conceptos adquiridos:	A través del desarrollo de la monografía se logró profundizar en los conceptos de ingeniería social y del uso de herramientas de recolección de información en fuentes públicas; estableciendo una guía para tener en cuenta por las personas y organizaciones para el endurecimiento de su seguridad. Adicionalmente se logró evidenciar que el OSINT no solo es usado por los ciberdelincuentes para obtener información, sino que es usado por periodistas, investigadores, países, grupos de hacker, ciberterroristas, Pentesting o ingenieros de hacking ético, pero el desconocimiento de estas herramientas hace que los países, empresas y personas no tomen en serio la seguridad al exponer datos sensibles en internet.
Conclusiones:	A partir del estudio realizado se puede concluir la falta de concientización y sensibilización de los usuarios frente a la información expuesta en internet que puede ser usada por los ingenieros sociales al momento de usar ataques de ingeniería social, una de las técnicas favoritas de los ciberdelincuentes es hacer uso del Phishing ya que pueden llegar a un sinfín de usuarios manipulando los sentimientos de las personas, adicionalmente el atacante puede lanzar un ataque dirigido a un usuario u organización en específico recopilando solo los datos de interés. Se hace evidente que, a través de herramientas de inteligencia de fuentes abiertas, un atacante puede perfilar un objetivo en específico y lanzar un ataque de ingeniería social, el

	desconocimiento de los usuarios al momento de realizar publicaciones en fuentes públicas crea falencias en la seguridad de las personas y empresas, se logra evidenciar que no son conscientes de en donde se encuentra la información. A partir del uso de herramientas OSINT, las empresas colombianas pueden identificar falencias en la seguridad de equipos y personas, claro está, que debe llevarse a cabo por el personal de seguridad, pues depende de ellos minimizar las vulnerabilidades halladas, previniendo los ataques de ingeniería social a través de capacitaciones al personal sobre el uso de las tecnologías de la información y las telecomunicaciones, la sensibilización y concientización al momento de exponer información en internet. Mediante las herramientas de OSINT, se logró visualizar el tipo de información que puede ser obtenida de fuentes públicas y puede ser usada por un ciberatacante con cualquiera de las técnicas o ataques de ingeniería social, pues sin la debida concientización, instrucción y capacitación de las personas se seguirá encontrando más información en internet, haciéndose un mundo propicio de información para los ciberdelincuentes. Mediante la guía se presentan diferentes sugerencias de seguridad para ser tenidas en cuenta por las empresas y usuarios colombianos, la aplicación de la guía permite prevenir la exposición de información sensible en fuentes públicas y fortalecer la seguridad personal y de la organización.