IDENTIFICACIÓN DE TÉCNICAS DE INGENIERÍA SOCIAL EJECUTADAS EN LA ENTIDAD EDUCATIVA ESAP HUILA

ING. REINALDO ENRIQUE RUIZ DUARTE
ING. JASSON FABIAN OLIVEROS ORTIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA, ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, COLOMBIA
2019

IDENTIFICACIÓN DE TÉCNICAS DE INGENIERÍA SOCIAL EJECUTADAS EN LA ENTIDAD EDUCATIVA ESAP HUILA

ING. REINALDO ENRIQUE RUIZ DUARTE
ING. JASSON FABIAN OLIVEROS ORTIZ

Monografía para optar el título de Especialista en seguridad informática

Director
John Freddy Quintero
Ingeniero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA, ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2019

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

AMENAZAS: Son las causas que se consideran potencial para generar un incidente no deseado, provocando daños en los sistemas[1].

ANTIVIRUS: Es un software que tiene como finalidad proteger el sistema operativo de los virus, supervisa en tiempo real eliminando o dejando en cuarentena el malware detectado[2].

CONTRASEÑA: Es una cadena de caracteres que tiene como finalidad la identificación ante un sistema el cual permite o restringe según el rol implementado. La funcionalidad es que el sistema compara el usuario con la contraseña en una lista almacenada en los servidores de la entidad; si la contraseña es correcta el sistema permite el ingreso, de lo contrario restringe el acceso[3].

EXPLOITS: Son programas intrusos que se valen de las brechas de seguridad de los sistemas, utilizando técnicas para atacar la red evadiendo las seguridades[4].

FIREWALL: Es un sistema de seguridad que tiene como función bloquear todo el tráfico malicioso en la red que se instala, mediante el bloqueo de puertos protege las conexiones no autorizadas a la red[5].

INGENIERÍA SOCIAL: Es una metodología que utiliza técnicas de engaño, su función es engañar al eslabón más débil que es el usuario para poder tomar acceso al sistema, unas de las técnicas que utiliza es el phishing el cual consiste en enviar correos spam, esperando que la víctima acceda al link que conlleva a la instalación de un malware que permite el control del equipo al atacante[6].

MALWARE: Son todos los programas informáticos que tienen la función de dañar el equipo tanto en software como hardware, entre ellos encontramos los virus, troyanos y gusanos. Su forma de reproducción es por medio de internet, USB, correos entre otros[7].

PHISHING: Esta técnica es utilizada por los ciberdelicuentes para poder acceder a un sistema valiéndose del poco conocimiento de seguridad del usuario, la técnica

---

[1] Guía para la Implementación de Seguridad de la Información en una MIPYME. [En línea]. Bogotá: MINTIC. 2016., 31 p. Disponible en: https://www.mintic.gov.co/gestionti/615/articles5482_Guia_Seguridad_informacion_Mypimes.pdf.
[2] Op. cit., p. 6
[3] Op. cit., p. 8
[4] Op. cit., p. 8
[5] Op. cit., p. 9
[6] BERMÚDEZ PENAGOS, Edilberto. Ingeniería Social, un factor de riesgo informático inminente en la universidad cooperativa de Colombia. Trabajo de investigación especialista en seguridad informática. Neiva. Universidad Nacional Abierta y a Distancia. Facultad de educación, 2015. 116 p
[7] Op. cit., p. 17

consiste en lanzar el ataque esperando a que el usuario caiga en la trampa, es similar a la pesca de ahí se deriva el nombre de phishing[8].

[8] Op. cit., p. 10

INTRODUCCION

Una noticia de la que se habla mucho por redes sociales, prensa, televisión y otros medios de comunicación, son los hurtos y extorsiones vía internet, de los cuales muchísimas personas son afectadas. En estos tiempos, los hurtos han evolucionado, permeando la plataforma digital haciendo que la seguridad de la información penda de un hilo y esta, aunque sea considerada mínima, cobran gran relevancia en los cibercriminales para realizar sus fechorías como lo son: los hurtos en bancas virtuales, la obtención de información clasificada entre otros, convirtiéndose este delito en el pan del día a día. Y todos estos sucesos hacen generar una pregunta que es casi obligada realizar, ¿Cómo puede suceder esto?, si se vive en una era donde los niveles de seguridad de las empresas se han incrementado, donde los sistemas informáticos se rigen por políticas de seguridad que pueden considerarse seguros. Es ahí donde la ingeniera social brinda la respuesta al interrogante formulado, los delincuentes informáticos se valen de cualquier recurso disponible para lograr sus propósitos, sumado a esto las personas no agregan mayor seguridad al manejo de su información o por lo menos a la que están involucrados en su diario vivir como los son: los datos de personas, familiares, conocidos, nombre de mascotas, actividades que hacen repetitivamente y sistemáticamente, las cuales pueden ser vigiladas por los delincuentes y utilizadas para crear patrones con los que buscan explotar y vulnerar en las victimas.

El presente trabajo investigativo busca que las personas que utilizan los servicios informáticos del ciberespacio entiendan el concepto de ingeniería social, su definición, su objetivo, y el por qué es posible que mucha de la información personal que se comparte en la internet pueda ser utilizada por los cibercriminales, comprendiendo así como estos seleccionan a qué tipo de personas enfocan sus ataques, de igual forma se busca generar más consciencia al momento de acceder a entregar datos personales buscando crear un modelo de cultura de prudencia cibernética.

Para esto, se agregaron conceptos que ayudaran a tener un enfoque general sobre la ingeniera social, se realizaron indagaciones sobre casos ocurridos en Colombia referentes a entidades educativas, se analizaron diferentes técnicas de ingeniera social y se promovieron los buenos hábitos en la seguridad informática. La población objeto de estudio para la presente monografía fue la Escuela Superior de Administración Publica ESAP territorial Huila entidad educativa ubicada en el municipio de Neiva, departamento del Huila en la cual se buscó atenuar los ataques por ingeniera social, analizando los ataques más utilizados por la ingeniería social, los perfiles de quienes pueden realizar dichos ataques, aprender a identificarlos y como poder evitarlos.

El progreso de la monografía se realizó en dos periodos académicos de la especialización de seguridad informática de la Universidad Nacional abierta y a distancia.

1 PLANTEAMIENTO DEL PROBLEMA

Actualmente y como lo manifiesta la página Colombia digital en la ingeniera social los usuarios son considerados el eslabón más débil dentro del circulo de custodia de activos informáticos[9], de nada vale tener en los sistemas sofisticados esquema de seguridad, e invertir en firewall y software de seguridad si un funcionario de la entidad no tiene la información y la capacitación necesaria para darle seguridad a su equipo y al acceso de este[10].

En Colombia los ataques más usados y que utilizan la técnica de ingeniera social se conoce como phishing (fraude informático que tiene como fin obtener usuarios y contraseñas, mediante suplantación de identidad por medio de correo electrónico SPAM[11]) de acuerdo al estudio presentado por la directora de ETEK internacional Patricia Gaviria esa modalidad de ataque aumentó en un 22.6% entre los años 2015 y el 2016, estimando un aumento a partir del 2017 entre 30 y 40% cada año[12].

De acuerdo a los resultados de la anterior investigación, se buscó que en la ESAP se identificaran los posibles focos de vulnerabilidad que podrían ocasionar problemas de ingeniería social y así capacitar al personal para que tenga mayor conocimiento y manejo sobre temas de seguridad de los posibles ataques y riesgos en los que pueden incurrir los funcionarios en la disponibilidad, confidencialidad e integridad de la información institucional.

Lo cual hace que surja la pregunta:

¿Qué tan expuesta podría estar la infraestructura tecnológica de la ESAP Neiva Huila, a los ataques informáticos mediante la modalidad de ingeniería social?

---

[9] CORPORACIÓN COLOMBIA DIGITAL. La ingeniería social: el usuario continúa siendo el eslabón más débil [en línea]. 2015., 1 p. [Citado 13-septiembre-2018]. Disponible en https://colombiadigital.net/actualidad/articulos-informativos/item/8556-la-ingenieria-social-el-usuario-continua-siendo-el-eslabon-mas-debil.html

[10] SANTOS CALDERÓN, Guillermo. Ojo a la ingeniería social [en línea]. Bogotá: El tiempo. 2018., 1 p. [Citado 13-septiembre-2018]. Disponible en https://www.eltiempo.com/opinion/columnistas/guillermo-santos-calderon/ojo-a-la-ingenieria-social-que-afecta-a-las-personas-217088

[11] Instituto nacional de ciberseguridad en España. Conoce a fondo qué es el phishing [en línea]. España: 2018. [Citado 13-septiembre-2018]. Disponible en https://www.osi.es/es/banca-electronica

[12] NOTICIAS RCN. Pishing, el método de robo por internet más utilizado en el país [en línea]. Bogotá: RCN. 2018. [Citado 13-septiembre-2018]. disponible en https://noticias.canalrcn.com/tecnologia-tecnologia/pishing-el-metodo-robo-internet-mas-utilizado-el-pais

2 JUSTIFICACIÓN

A través de los tiempos, en la humanidad se han generado cambios que han permitido una evolución y con ella un desarrollo de todas las actividades generadas por el hombre, esto ha traído consigo la necesidad de suplir todas estas actividades, y sin duda alguna ha sido la tecnología quien más ha aportado a estos cambios, emprendiendo una dura tarea cada día con el fin de ir a la vanguardia y optimizar todos los procesos en este desarrollo; Es factible que la utilización de estas herramientas consideradas como potentes puedan cambiar la sociedad. Para la seguridad en los automóviles los microchips cumplen con la funcionalidad de automatizar y asesorar la conducción. Otra herramienta fundamental es la realidad virtual que bajo su implantación ayudará a todas las áreas en la simulación de procesos para su debido estudio[13].

En este sentido la ingeniería social juega un papel preponderante convirtiéndose en esa técnica utilizada por quienes han hecho de la tecnología un medio para generar todo tipo de actividades fraudulentas, sacando provecho a través de su conocimiento atacando a un eslabón débil en la seguridad informática[14], las personas ingenuas e incautas y así extraerles información confidencial y relevante (cuentas bancarias, redes sociales, bases de datos, usuarios, contraseñas, etc.) y de esta manera generar mecanismos de presión, extorción, manipulación de la información y todo lo necesario para establecer un escenario propicio para sus objetivos personales afectando la entereza de la información en las compañías, instituciones u organizaciones.

Por tal motivo es transcendental exaltar que los datos son el activo más importante para las instituciones y corporaciones junto con los recursos humanos, es importante la conducción de la información ya que esto puede significar el triunfo o fracaso de la entidad que busca la sostenibilidad y crecimiento[15], y se debe aplicar las normas de seguridad adecuadas para la protección, teniendo en cuenta los posibles ataques identificando las técnicas que se aplican para sustraer información confidencial[16] .

---

[13] EL TIEMPO. Tecnologías evolución y futuro [en línea]. Bogotá: 2018. Disponible en https://m.eltiempo.com/archivo/documento/MAM-219859

[14] STOLK, Alejandra. Triángulo de debilidades del sistema [en línea]. Bogotá: Es la red. 2013., 40 p. Disponible en http://www.human.ula.ve/ceaa/temporal/fundamentos_de_seguridad.pdf

[15] COHEN KAREN, Daniel. Importancia de la información para las empresas [En Línea]. Argentina: 2018. Disponible en https://www.grandespymes.com.ar/2014/10/03/importancia-de-la-informacion-para-las-empresas/

[16] HANSEN, Denis. SAVE Social Vulnerability & Assessment Framework [en Línea]. 2017., 42-49 p. Disponible en http://www.fak.dk/publikationer/Documents/Project%20SAVE.pdf

Mediante los resultados obtenidos se confirma la utilidad de generar una cultura en seguridad informática y prevenir futuros ataques mediante la modalidad de la ingeniería social que pueden presentar las instituciones educativas.

Entendiendo que la ESAP territorial Huila es una entidad de educación superior de una gran trayectoria en el sector público y que por lo mismo no es ajena a dichos ataques informáticos a través de la ingeniería social, se identificaran los diferentes tipos de ataques a los que hayan podido estar expuestos y la seguridad debe ser un tema implementado en todas las dependencias del campus universitario y no solo en la oficina de tecnología informática como muchos pueden pensar.

Al tener el conocimiento de la problemática de la Institución, es determinante que los administrativos y directivos tengan claro cuán importante es la seguridad de los activos informáticos y le brinden la relevancia que esta debe tener, por ende es necesario abordar estos temas con mayor frecuencia ya que la entidad puede ser víctima de un ataque, de igual forma se hace necesario identificar cual es el personal más vulnerable, evaluando su conocimiento sobre el tema de la seguridad de la información, y que puedan relacionar que los aspectos que son desarrollados en su labores diarias están enfocados a la problemática investigada; la propuesta de este trabajo no es novedosa pero si muy efectiva a la hora de recoger información dando un alto impacto sobre la recolección de información en los ambientes laborales de la empresa.

Por tal motivo es importante reconocer que la información en la entidad ESAP Huila es un activo muy valioso como lo es el recurso humano, por tal motivo a los segundos se les debe ofrecer la defensa de la información, para así resguardarla sobre cualquier tipo de arremetida, por otro lado sabiendo que la información es importante, existirán personas que quieran alcanzarla de forma no autorizada, en este sentido es imperioso identificar las debilidades de los sistemas de seguridad de la institución frente a todo tipo de amenazas.

Es vital que el personal de la entidad reconozca las posibles formas en que puede ser vulnerada la información mediante la utilización de la ingeniería social, esto creará una cultura responsable frente a este tipo de temas, y los llevará alcanzar un nivel de conciencia lo que automáticamente elevará el nivel de seguridad en el personal, convirtiendo en un valor agregado la integridad, disponibilidad y confidencialidad de la información dentro de la organización

3 OBJETIVOS DEL PROYECTO

3.1 OBJETIVO GENERAL

Analizar la infraestructura tecnológica y los ataques de ingeniería social más frecuentes en la entidad ESAP Huila.

3.2 OBJETIVOS ESPECIFICOS

- Identificar los ataques informáticos realizados por ingeniería social en la entidad educativa ESAP HUILA.
- Describir las consecuencias de un ataque informático por medio de ingeniería social en la entidad ESAP HUILA.
- Proponer una infraestructura tecnológica que permita detener los ataques informáticos en la entidad ESAP HUILA.
- Hacer recomendaciones buscando crear hábitos de seguridad en los empleados para lograr reducir los ataques por ingeniería social en la entidad ESAP HUILA.

4 MARCO TEORICO CONCEPTUAL

Las diferentes organizaciones buscan la seguridad y protección de sus activos informáticos, porque saben que son parte fundamental de su patrimonio, es por ello que cuidan que la información que se encuentra en su instalaciones cuenten con programas que les proporcione un alto grado de seguridad, olvidando casi que por descuido, que estos software son controlados por seres humanos que al no ser capacitados en estos temas se convierten en un problema de seguridad informática, pues son ellos quienes terminan seleccionando por claves de seguridad el nombre de alguno de sus hijos, su fecha de nacimiento, o el nombre de su mascota, convirtiéndolos así en el eslabón más débil de la cadena de custodia,.

El presente trabajo pretende identificar las técnicas de ingeniería social que se están utilizando en la Escuela Superior de Administración Publica ESAP, que están relacionadas con dos conceptos que debemos tener claro como lo son: **seguridad de la información y seguridad informática** y para ello se debe encontrar las diferencias entre estos términos, entendiéndose que la seguridad de la información se define como las diferentes medidas y técnicas que logran en la organización mantener la integridad, disponibilidad y confidencialidad de un sistema de información[17], mientras que la seguridad informática se centra en procesos técnicos que permite preservar la información manteniendo la integridad, disponibilidad, confidencialidad incluyendo la responsabilidad, el no repudio y la fiabilidad[18], la clara diferencia está en que la seguridad informática es un concepto más completo que da mayor profundidad a temas de seguridad mientras que la seguridad de la información se preocupa porque el otro se pueda desarrollar sin problemas.

Para poder hablar de ingeniería social hay que entender conceptos que son trascendentales, que hacen parte de la seguridad y se debe tener en cuenta como lo son:

Confidencialidad: Se define confidencialidad cuando la información está disponible solo a las personas autorizadas, bajo las situaciones y contextos que se constituyen

[17] MIFSUD, Elvira. Seguridad de la información / Seguridad informática [en Línea]. España: 2012., 2 p. [Citado 15-septiembre-2018] Disponible en http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

[18] Ibíd., p.4.

en la entidad. Es de informar que bajo ninguna circunstancia se puede obtener la información a no ser que este establecido en las políticas de seguridad[19].

Integridad: Se debe garantizar que la información mantenga en su estado original sin ser alterada a no ser por autorización.[20] Es importante para la entidad mantener con exactitud la información generada sin importar el medio, con el fin de garantizar transparencia en los procesos que se llegue a solicitar.

Disponibilidad: Es la cualidad de la información de brindar accesibilidad al personal acreditado en el momento solicitado. Es garantizar que las revisiones de seguridad que se efectúan en los sistemas de información deben de estar en perfecto funcionamiento, permitiendo la disponibilidad de la información.

No Repudio: es una cualidad que pueden brindarse desde el origen o el destino, en el origen el emisor no puede negar el envío porque el receptor tiene pruebas o viceversa. En toda transacción, existe un receptor y un emisor encargados de mantener la confianza entre él envió del mensaje con el fin de evitar intercepción por un tercero. [21]

El objetivo principal de la seguridad de la información como se puede observar en la Figura 1, es mantener las características de: disponibilidad en el momento de acceder a la información, integridad en el momento de validar los datos y confidencialidad en el momento de divulgar la información.

Figura 1 Confidencialidad integridad y disponibilidad

Fuente: https://infosegur.files.wordpress.com/2013/11/unidad-1.jpg

[19] VOUTSSAS, Juan. Preservación documental digital y seguridad informática [en línea]. México: 2010. [Citado 15-septiembre-2018]. Disponible en http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

[20] STANLLING, William. Comunicaciones y Redes de Computadores. 7 ed. México: Prentice Hall 2004
SANTOS COSTAS, Jesús. Seguridad informática. Editorial y Publicaciones, 2010.

La ingeniería social es un método que puede utilizarse en muchos ámbitos de la vida, para poder conceptualizarla se debe entender la definición de cada termino por separado, por ejemplo el término social se define como lo relativo o perteneciente a la sociedad[22] y que sociedad se deduce como el vínculo de personas que interactúan entre ellas mismas compartiendo una misma cultura para conformar una comunidad.[23] Por otro lado se entiende por ingeniería según la Ley colombiana 842 de 2003 "toda aplicación de las ciencias físicas, químicas y matemáticas; de la técnica industrial y en general, del ingenio humano, a la utilización e invención sobre la materia"[24], fusionando estos conceptos se pueden entender que la ingeniera social es según Torres Ariel,[25] la ciencia de entender y manipular de forma habilidosa a los seres humanos para que operen de cierta forma en ciertos aspectos de la vida cotidiana.

La ingeniería social se utiliza muy a diario y como manifiesta el blog Enter.com en su artículo la ingeniería social: el ataque informático más peligroso "esta puede ser aplicada a cualquier persona desde niños incautos hasta grandes políticos de la sociedad"[26], un ejemplo de ellos es lo que cotidianamente realiza un paciente cuando visita a su doctor, el doctor realiza preguntas a su paciente con el fin de obtener información de los hábitos y costumbres de la persona atendida, todo lo realiza con el fin poder sacar un cuadro clínico sobre su patología que sumado a los exámenes realizados previamente el medico pueda emitir un concepto sobre su estado de salud, se puede decir que es la suma de múltiples habilidades que cuando se unen puede hallar una problemática que no se podía encontrar o deducir fácilmente, en otros palabras como lo manifiesta Durigon (2016)[27], ingeniera social se puede entender como la suma de información acción e ingenio.

De acuerdo a la anterior definición se podría decir que la ingeniería social desde otro contexto es "la manera sutil y engañosa que utilizan los ciberdelicuentes para poder acceder a la información requerida de una forma rápida y segura,

[22] PÉREZ PORTO Julián y MERINO, María. Definición de social [en línea]. 2009., 1 p. [Citado 25-septiembre-2018]. Disponible en https://definicion.de/social/
[23] Ibíd., p. 1.
[24] EL CONGRESO DE COLOMBIA. Ley 842 del 14 de octubre de 2003, Artículo 1. P 1. Concepto de ingeniería.
[25] TORRES, Ariel. Hackearán tu mente: Los trucos de ingeniería social que los piratas informáticos usan para cometer fraude, secuestrar archivos y robar tu identidad. Argentina: Grupo Planeta
[26] ENTER: CO. La ingeniería social: el ataque informático más peligroso [en línea]. 2018. [Citado 25-septiembre-2018]. Disponible en http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/
[27] DURIGON, Néstor (2016). Grandes maestros de la estafa. Argentina: Penguin Random House grupo editorial argentina

manipulando a las víctimas para obtener la información confidencial de la organización o del individuo"[28].

Por lo anterior la ingeniería social ha tenido una evolución importante desde la seguridad informática, según el instituto nacional de seguridad INCIBE "se ha logrado posicionar como una las principales herramientas que usan los Ciberdelincuentes para captar información y hacerse a las debilidades que tienen los seres humanos por naturaleza"[29], realizar un ataque por ingeniera social se puede lograr de muchas formas, una de ellas según en la página web de seguridad welivesecurity,[30] se puede realizar por medio de llamadas telefónicas donde se imita la voz de un funcionario del banco el cual pide información supuestamente de verificación o actualización para corroborar los datos que el banco tiene sobre la víctima, todo esto con el fin de que el atacante logre tener acceso a sus cuentas bancarias, tarjetas de créditos, redes sociales y correos electrónicos, otra forma de ingeniería social la propone la revista tecnológica BYTE[31]en donde se aplica por medio de correo falso o lo que también se ha llamado en la actualidad phishing, envían información diciendo que es el feliz ganador de una cuantiosa suma de dinero, y que para poder realizar el trámite de este, debe realizar un aporte significativo y esperar que hagan el desembolso, dentro de esta misma modalidad[32] están los correos que invitan a entrar a páginas falsas como el banco, donde piden que registre o actualice los datos personales porque ya se encuentran desactualizados.

La ingeniería social es utilizada para permear al recurso humano de las empresas, la revista de seguridad informática de la universidad UNAM de México[33], argumenta que el usuario es manipulado con una serie de preguntas con el propósito de indagar y obtener datos confidenciales de las organizaciones, así como también existen empleados que cuentan con poco conocimiento sobre temas informáticos y sobre su importancia. A pesar que se conoce el riesgo que generan los ataques por la ingeniería social y la falta de la elaboración y aplicabilidad de políticas de seguridad, las directivas no asumen el costo de realizar la implementación de la

[28] INCIBE. La ingeniería social en la empresa: aprovechando la naturaleza humana [en línea]. España: 2014. [Citado 28-septiembre-2018]. Disponible en https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-en-empresas
[29] TECTECO. Qué es la ingeniería social y cómo afecta a la ciberseguridad [en línea]. España: 2018. [Citado 28-septiembre-2018]. Disponible en https://www.tecteco.com/que-es-la-ingenieria-social-y-como-afecta-a-la-ciberseguridad/
[30] WELIVESECURITY. 5 cosas que debes saber sobre la Ingeniería Social [en línea]. 2016. [Citado 28-septiembre-2018]. Disponible en https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/
[31] REVISTABYTE. La mitad de ataques de phishing es financiero [en línea]. 2018. [Citado 28-septiembre-2018]. Disponible en https://www.revistabyte.es/actualidad-byte/ataques-phishing-financiero/
[32] Ibít., 1 p.
[33] SANDOVAL CASTELLANOS, Edgar. Ingeniería social: corrompiendo la mente humana [en línea]. México: Revista. Seguridad. 2010. [Citado 28-septiembre-2018]. Disponible en https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-hum ana

seguridad de la información, ya sea por motivos económicos o por falta de concientización.

Desde lo práctico hablar de ingeniera social se puede traducir en un simple mensaje que llega por internet, una llamada telefónica donde solicitan datos personales, con el fin de engañar y sacar información, fingir ser el empleado de una compañía o un colega de trabajo en otra sede, un cliente, un operario de servicio; desde internet enviar link de acceso de publicidad vistosa y seductora al usuario incauto donde se busca que la víctima revele información, o peor aún que entregue información sensible de una empresa, y así buscar explotar las debilidades naturales de las personas.

"Los empleados a menudo abren archivos desconocidos, hacen clic en enlaces sospechosos e incluso se comunican con los atacantes. En el 88% de los casos, estos empleados son demasiado confiados trabajaron fuera de TI (como contadores, abogados y gerentes). Una cuarta parte de estos empleados eran supervisores de equipo. Sin embargo, nadie está exento a los errores, y el 3% por ciento de los profesionales de la seguridad también caen en este tipo de engaño."[34]

Espitia (2018) explica, que la manera de poder realizar una disminución de los ataques por ingeniera social en las empresas[35] es concientizar a todo el recurso humano de la importancia de la seguridad, realizar capacitaciones periódicas y constantes sobre las diferentes modalidades que utilizan en la ingeniería social, todas las personas de la compañía sin distinción alguna desde el mensajero, secretaria hasta los gerentes o accionistas que forman parte de la organización, por ende son responsables de cuidar los activos más valiosos de la organización como son los datos. El ministerios de las Tics en Colombia, con su técnica de capacitación, sensibilización y comunicación de la seguridad de la información Min TIC[36] plantea que estas capacitaciones se debe divulgar con los empleados sobre las formas, métodos y debilidades que se utilizan para poder permear la seguridad de cada individuo y así con esta información lograr identificar cuándo y dónde se está intentado realizar un ataque por ingeniera social y así lograr dar aviso ante esta anomalía al personal directamente encargado.

[34] DIGITAL SECURITY. La ingeniería social sigue estando detrás de demasiados ataques [en línea]. 2018. [Citado 31-septiembre-2018]. Disponible en https://www.itdigitalsecurity.es/actualidad/2018/04/la-ingenieria-social-sigue-estando-detras-de-demasiados-ataques

[35] ESPITIA, Angélica. Ingeniería social amenaza latente para la seguridad informática [en línea]. Bogotá: 2018, 4 p. [Citado 31-septiembre-2018]. Disponible en http://polux.unipiloto.edu.co:8080/00001891.pdf

[36] MINTIC. Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información [en línea]. Bogotá: 2016., 15-30 p. [Citado 31-septiembre-2018]. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

Dichas capacitaciones pueden iniciar con el personal de TI (Tecnología de la Información), convirtiéndose en los precursores y aplicadores de la filosofía y el estilo de vida seguro en cuanto a la información se refiere, retransmitiendo y retroalimentando constantemente los conocimientos adquiridos a todas las áreas de la empresa, estas retroalimentaciones se deben realizar en pequeñas capacitaciones didácticas donde se muestre a los trabajadores como reducir las amenazas y creando ambientes seguros de trabajo, logrando con el tiempo crear una cultura de capacitación por personal interno de la TI y así contribuir a disminuir los recursos que la empresa destinaba en capacitaciones externas sobre estos temas de seguridad.

Figura 2 Formas de ataque por ingeniería social

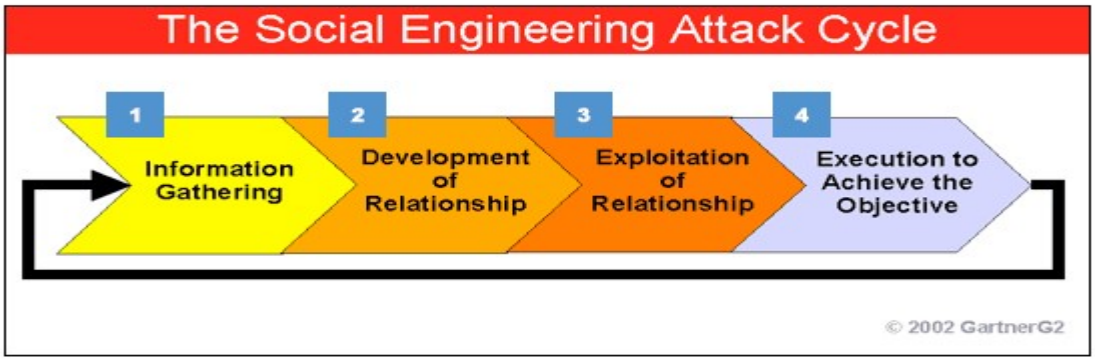
Fuente: *https://4.bp.blogspot.com/-fILBd5iyf2I/WTBLeeIfufI/AAAAAAAAGJo/HV_41MkyiDEw3GZr4dS3sw7maigPoSOAACLcB/s1600/ingenieria-social1.png*

4.1 METODOLOGÍA DE UN ATAQUE POR INGENIERÍA SOCIAL

La ingeniera social como técnica de ataque no es indiferente a cualquier otra forma de ataque informático que como tal responde a una metodología básica de funcionamiento que es seguir a las víctimas para poder cumplir con el objetivo de

conseguir la información, a continuación se describirán los pasos a seguir basados en la propuesta de estudios de la metodología de ingeniería social[37] que se utilizan para describirla, la Figura 3 describe el período de ataque de una intrusión por ingeniería social en 4 pasos: Selección y reconocimiento, Análisis y contacto, Generación de vector de ataque y explotación y ejecución de vector de intrusión.

Figura 3. Ciclos de un Ataque por Ingeniería Social



Fuente: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf

4.1.1 Selección y reconocimiento. Se utiliza una técnica denominada *Footprinting* la cual tiene como propósito reunir información de la víctima – objetivo utilizando como medio un sitio web clonados para sustraer información, en este paso es muy importante conocer el escenario que se pretende atacar. Para esta fase es muy importante crear un perfil de la víctima, identificar sus hábitos, vida, su nivel de intelectualidad, su nivel de confianza ante la gente, su nivel de conocimiento informático y demás**.**

4.1.2 Análisis y contacto. Con los datos recolectados en el ítem anterior, se realiza un análisis minucioso, se busca hacer contacto con la víctima para crear un vínculo afectivo con ella y avanzar a una relación de confianza, con el fin de que sea revelada la información a la que se quiere acceder.

4.1.3 Desarrollo de la estrategia de ataque y explotación. Creado el lazo de amistad que nació seguido de efectuarse la fase de selección y reconocimiento, de análisis y contacto, el usuario está susceptible a una manipulación. Ya se puede

[37] BERENGUER SERRATO, David y GARCÍA VALDÉS, Ángela. Estudios de la metodología de ingeniería social [en línea]. España: 2018. [Citado 31-septiembre-2018]. Disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf

generar el ataque de suplantación de identidad y robo de información dando paso a la última fase ejecución de vector e intrusión.

4.1.4 Ejecución de la estrategia e intromisión. Luego de cumplidas las fases de selección, reconocimiento, análisis, contacto, la generación del vector de ataque y explotación; La información es obtenida y los datos del objetivo están vulnerados, logrando dar acceso a la cuenta, sistema, red etc., que se planeó atacar. Es importante reconocer e identificar cada etapa que conforman la ingeniera social, ya que esto brindará la ventaja de identificar en que paso considera el atacante que se encuentra con la finalidad de aprender cuáles son sus tácticas sin subestimar su inteligencia y mentalidad, es también importante aprender y aprovechar ese conocimiento para mejorar las habilidades de entendimiento hacia los atacantes.

Es importante conocer aún más sobre temas referentes a la ingeniería social ya que existen dos tipos de ataques: los que son basados en la tecnología y los que son basados en engaños enfocados al usuario. Cada uno tiene diferentes niveles de aplicabilidad, a saber:

4.2 BASADOS EN LA TECNOLOGÍA

Son aquellos donde se utiliza cualquier medio tecnológico informático, con el objetivo de realizar el engaño. Ya sea por medio de una aplicación o un sistema alterado por el atacante o denominado hacker, algunas de las técnicas de tecnología utilizadas en la ingeniería social basados en la tecnología se describen a continuación:

4.2.1 Phishing: Método utilizado que consiste enviar correos o sitios web falsos con el fin de obtener información y realizar estafas. Estos correos suelen hacer creer a las víctimas que son fuentes fiables como entidades bancarias y el único fin que buscan es conseguir información confidencial del usuario para posteriormente realizar algún tipo de fraude[38].

Figura 4 Ataque por phishing

[38] MÉNDEZ, Belisario y NORILEY, Aymara. Análisis de Métodos de Ataques de Phishing. Trabajo de grado en seguridad informática. Argentina: universidad de buenos aires. Facultad de ciencias económicas. 2014. 61 p.

Fuente: https://www.welivesecurity.com/la-es/2017/04/21/correo-de-visa-phishing/correo-falso-visa/#single-post-fancybox

4.2.2 Email con Código Malicioso. El correo electrónico de forma adjunta puede cargar archivos que tienen código malicioso conocidos como malware y pueden dañar el sistema o causar un mal funcionamiento, se debe tener un cuidado especial con este tipo de email, ya que su principal objetivo es crear brechas de seguridad o puertas traseras que permiten el robo de información o datos, infectar el equipo con un malware que permitirá al atacante tener acceso a la información.

"El Propósito del atacante, es insertar de forma eficaz en el equipo de la víctima software con código malicioso o los también llamados spyware, que se define como (spy = espía) (ware = software) y después de su instalación, capturar la información en el momento que la víctima introduzca usuario y password, o cuando realice cualquier tipo de transacción financiera, una compra o pago por Internet"[39]. La figura 4 Muestra la estructura de un email con código malicioso.

4.2.3 Spam. Este tipo de correo son considerados los correos basura o también son llamados correos no deseados que normalmente son enviados por remitentes desconocidos y que pueden tornarse molestos, este tipo de correos se generan cuando se suscriben a páginas web para solicitar información y estas plataformas o

[39] NORFIPC. Evitar la infección por virus o malware a través del correo electrónico [en línea]. 2018. [Citado 31-septiembre-2018]. Disponible en https://norfipc.com/virus/evitar-infeccion-virus-malware-email-correo-electronico.html

páginas actúan sobre las cuentas de correo, enviando promociones o novedades sobre sus productos, estos emails spam se pueden filtrar con código malicioso.

"en definitiva, las direcciones electrónicas son hurtadas, adquiridas, recogidas en la web o tomadas de cadenas de mail; Aunque hay algunos spammers que envían solamente un mensaje, también hay muchos que bombardean todas las semanas con el mismo mensaje que nadie lee. La mayoría de las veces si la victima contesta el mail pidiendo ser removido de la lista, lo único que hace es confirmar que su dirección existe. Por lo tanto, es conveniente no responder nunca a un mensaje no solicitado.."[40].

4.2.4 Ventanas emergentes. "O ventana pop-up es el contenido que se genera en las ventanas de navegadores o pestañas de Windows donde la información que un usuario no ha solicitado le llega, este tipo de ventanas con información por lo general con publicidad sobre un producto siempre aparece de forma repentina en un navegador web o en la pantalla del ordenador. Lo que busca es mostrar información complementaria, que consiga enviar información de interés o que por el contrario busque reflejar publicidad sobre una marca o negocio"[41] estos mensajes pueden ser portadores de infecciones con código malicioso "malware", virus, troyanos o solamente se convierten en avisos perturbadores al abrir constantemente ventanas del navegador y mostrar publicidad; Cabe anotar que la mayoría de los navegadores de forma nativa incluyen bloqueadores para las ventanas emergentes o los pop-up.

4.3 BASADO EN EL ENGAÑO HUMANO

Es una técnica de la ingeniería social que busca aprovechar las características que definen y hacen única a cada persona: el fisgoneo, el temor, la codicia, la concupiscencia, la ternura, etc. son usadas con el único objetivo de obtener datos sensibles y confidenciales de la víctima y así vulnerar los sistemas. Esta técnica pueden pasar desapercibida para personas sin la capacitación o el entrenamiento adecuado, emplea así "vulnerabilidades en la conducta humana y comúnmente se utiliza en personas con cierto nivel de autoridad en las empresas"[42].

[40] SEGURIDADPC.NET. Concepto de spam [en línea]. 2016. [Citado 31-septiembre-2018]. Disponible en http://www.seguridadpc.net/spam.htm
[41] NEOATTACK. Concepto de Pop-up [en línea]. Barcelona: 2018. [Citado 03-octubre-2018]. Disponible en https://neoattack.com/neowiki/pop-up/
[42] SCOTT SPENCER, James. Ingeniería Social: eludiendo el "firewall humano" [en línea]. México: 2011. [Citado 03-octubre-2018]. Disponible en http://www.magazcitum.com.mx/?p=1173#.W_3bvGhKjIW

4.3.1 Suplantación de identidad. Se entiende como "aquel ejercicio por medio del cual un individuo se hace pasar por otro, para realizar acciones de carácter ilegal, como solicitar aprobaciones de crédito o préstamo hipotecario, contratar servicios telefónicos o realizar ataques contra otros individuos."[43] Un ejemplo de esto puede ser cuando por medio de una llamada telefónica llaman a la empresa, se hacen pasar por un usuario legítimo y solicitan cambios de clave de los correos o equipos de cómputos

4.3.2 Dumpster Diving ó Trashing. Esta técnica denominada también Búsqueda en la basura es una técnica muy usada, aunque por su nombre suene algo extraño, se trata de encontrar en los botes de las basuras parte de los desperdicios, documentos desechados con información valiosa para su uso y divulgación, este tipo de basura se puede conseguir datos financieros, información de recibos públicos, números telefónicos etc. Para evitar esta técnica es recomendable que tanto como las personas del común como en las organizaciones trituraren todo el papel que se genera y seguir protocolos de seguridad con todo el documento que vaya a ser desechado.

4.3.3 Shoulder Surfing. Técnica basada en espiar por encima del hombro, utilizada por aquellos que atacan con ingeniería social, solo es necesario estar ubicado estratégicamente en donde concurre mucha gente, como son bancos, cajeros o sitios públicos como plazas o bibliotecas, y capturar visualmente lo que la víctima digita o escribe. En la actualidad se utilizan también programas en dispositivos móviles o cámaras para espiar y tomar fotografías de la pantalla o monitor, con el fin, de obtener claves de acceso al sistema, contraseñas, datos, números pin y datos similares con los que el cibercriminal pueda tener acceso a información privilegiada de otros usuarios sin su consentimiento, un ejemplo de ello lo ilustra la siguiente figura.

Figura 5 Shoulder Surfing

[43] LEGALITAS. Suplantación de identidad [en línea]. España: 2016. [Citado 03-octubre-2018]. Disponible en https://www.legalitas.com/actualidad/suplantacion-de-identidad

Fuente:
https://www.confirmasistemas.es/documentos_web/listado_contenidos/135/1/thumbs_web/c_24_401.jpg

4.3.4 Reverse Social Engineering. "La ingeniería social inversa, se trata de manifestar cómo está hecho un sistema percibiendo cómo es el proceso funcional y las características que este posee. El objetivo es adquirir la mayor cantidad de datos técnicos de un producto del cual no se tiene ningún tipo de información referente tanto a temas de diseño como de sus modelos o esquema interno de este"[44].

También es usada por los atacantes para ocasionar problemas o dificultades en las redes de comunicación o servicios de las empresas teniendo un conocimiento previo sobre la misma, luego ofrece sus servicios para solucionar el problema. Seguidamente el atacante al resolver el problema crea confianza y hace que las victimas siempre estén dependiendo del atacante para dar solución a los problemas de seguridad que se encuentren en la organización[45].

En esta técnica, es necesario precisar que implica mucho tiempo y dedicación por parte del ingeniero social o atacante, ya que debe socializar fácilmente con los usuarios de la empresa ganando su confianza, tener buen aspecto físico y aparentar ser de carácter inofensivo, y sobre todo tener un perfil bajo, así como ser siempre amable y sonreír para tener el agrado de la gente y del personal de las empresas[46].

4.3.5 Pretexting. Es un método donde el atacante se hace pasar por otra persona ya sea pública o enrolada en el negocio a vulnerar, para poder generar confianza a la víctima y lograr el objetivo de extraer la información. "Consiste en la forma de capturar datos y documentos contactando a una empresa y simular ser una determinada persona, con el fin de ser utilizada con actos delictivos"[47].

4.3.6 Tailgating. Esta técnica se fundamenta en requerir auxilio directamente de una persona con acceso en áreas sensibles de la compañía, utilizando RFID

[44] SEGURIDAD INFORMATICA ELLA. Ingeniería social inversa [en línea]. 2017. [Citado 03-octubre-2018]. Disponible en http://seguridadinformaticaeya.blogspot.com/2017/03/ingenieria-social-inversa.html
[45] JARAMILLO HINOJOSA, Lucia. Estudio del grado de incidencia de la ingeniería social en la primera fase de los ataques informáticos que se realizan actualmente en las empresas privadas del ecuador. Ecuador.
[46] MOINELO, Lino. Ingeniería social inversa [en línea]. 2010. [Citado 03-octubre-2018]. Disponible en http://cualeslarealidad.blogspot.com/2010/03/ingenieria-social-inversa.html
[47] RED SEGURIDAD. ¿Pretexting? los ciberdelincuentes utilizan el teléfono para robar información confidencial [en línea]. 2013. [Citado 03-octubre-2018]. Disponible en http://www.redseguridad.com/actualidad/info-tic/pretexting-los-ciberdelincuentes-utilizan-el-telefono-para-robar-informacion-confidencial

(identificación por radiofrecuencia), biométrica o algún otro método de identificación. Esta técnica se utiliza cuando se hacen pasar por personal de mantenimiento de la empresa para poder acceder áreas restringidas, esta técnica es muy utilizada cuando identifican que las empresas tercerean ciertos servicios como el mantenimiento sobre todo cuando las empresas son demasiado grandes[48].

4.3.7 Deceptive relationships. En esta técnica el atacante busca crear un lazo personal para obtener datos importantes de la víctima o de un sistema en general. Para este ataque solo es suficiente entablar una conversación con la victima crear ciertos patrones de afinidad como gustos, por la música, deporte, autos etc., luego de creado el vínculo intentar extraer información que sea importante para el atacante como direcciones de teléfono sitios de ubicación teléfonos y demás y luego utilizar esta información para atacar a la víctima.

4.4 TIPOS DE ATACANTES

Para este apartado, se logrará hacer una profundización sobre las personas que están detrás de los tipos de ataques, aquellas que se consideran los cerebros de la operación, los que están detrás de las penetraciones a los sistemas y los que aprovechan todas las fallas que encuentran con sus vulnerabilidades.

Dentro de la clasificación existen diferentes roles, aunque ellos comúnmente se identifican como “hackers” es cierto que cada uno se identifica con su propio estilo y forma de realizar sus ataques y así de acuerdo a esto su forma de vulnerar los sistemas de información.

4.3.1 Ciberdelincuentes. Así como en el mundo normal existen los delincuentes, en la informática existen los ciberdelincuentes; estos son personas que realizan actos delictivos por medio de la internet con el fin de realizar ataques a sistemas de información, fraudes o publicar información confidencial o ilegal, el único objetivo es estar siempre en el ámbito ilegal y sacar provecho económico de sus actos delictivos. Según Andrés Galindo, director de Negocios y alianzas estratégicas de digiware hay siete rasgos para identificar a un delincuente informático.

1. Son personas que se destacan por poseer conocimiento importante en temas de informáticos e interconexiones de equipos

[48] GF0S.COM. Tailgating: acceso a zonas restringidas [en línea]. 2016. [Citado 03-octubre-2018]. Disponible en https://gf0s.com/2016/08/05/tailgating-acceso-a-zonas-restringidas/

2. Personas con conocimientos avanzados de usos de software especiales de no fácil manipulación por un individuo promedio
3. Personas que siempre están indagando en busca de obtener información de las reuniones sociales o conglomerado de personas
4. Persona que instala en equipos ajenos sin autorización programas de código malicioso para espiar movimiento y capturar información
5. Sujetos que no usa o inhabilita el software antivirus en su estación de trabajo
6. Persona que obtiene acceso de los equipos y utiliza los equipos sin el consentimiento de los miembros de la organización
7. Individuo que trabaja en horas no laborales dentro de la empresa sin dar una justificación laboral."[49]

4.3.2 Hackers. Persona con conocimientos avanzados en sistemas, informática y telecomunicaciones que los usa para poder realizar penetraciones, con el fin de acceder a sistemas informáticos sea por satisfacción personal, fortalecer los sistemas o realizar robos y fraudes sobre estos, estos se encuentran en una delgada línea donde ellos son los que deciden sin son simplemente observadores, dar el conocimiento adquirido para fortalecer los sistemas o atacar esas debilidades encontradas.

"Este concepto está estrechamente relacionado con el origen de la internet en la que fueron previstas oportunidades de crecimiento social y económico entre los años 60 y 70. Desde su comienzo militar (como DARPA) hasta su propagación extendida a partir del año 2000 y su implantación global, hoy en diversos dispositivos electrónicos (desde laptop, Desktop hasta servidores, Smartphone, tabletas…). Internet ha servido como un medio de transporte para dar popularidad, multiplicar mensajes, intercambiar información para este tipo de movimiento el término que se utilizaba inicialmente era "hack" cuya definición "perder el tiempo"; con el paso de los años el término ha ido cambiando sobre todo en el contexto informático."[50]

4.3.3 Crackers. Persona que se dedica a realizar cambios en los sistemas licenciados para darle un uso no autorizado rompiendo contraseñas, sistemas de validación y de encriptación. Son las personas que se dedican a realizar programas para alterar o burlar la seguridad de algún programa con licencia paga, se dice además que es un derivado del hacker, pero a diferencia de estos su fin siempre se basa en alterar o dañar un sistema informático, hay personas que lo hacen por fines económicos, otros simplemente por ganar el crédito.

[49] GESTION. Siete características para identificar a un ciberdelincuentes [en línea]. 2016. [Citado 09-octubre-2018]. Disponible en https://gestion.pe/tecnologia/siete-caracteristicas-identificar-ciberdelincuente-122640

[50] ROSE, Karen. LA INTERNET DE LAS COSAS— UNA BREVE RESEÑA. Cuestiones relacionadas con las economías emergentes y el desarrollo [En línea]. 2015. [Citado 28-octubre-2018]. Disponible en https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf

4.3.4 Spammers. Son las personas que se dedican a enviar correos masivos no deseados a personas o empresas con información comercial o para redireccionar a páginas falsas con el fin de saturar bandejas de correo y obtener información de los usuarios. Estos individuos almacenan correos en bases de datos propias que adquieren ya sea por la compra en internet o aprovechando robots que almacenan siempre los hilos de correos que se van generando cuando el correo es reenviado.

4.3.5 Sniffers. Persona que se conecta a las redes con el objetivo de captar todo el tráfico que se genera sobre este, con el fin de capturar y desencriptar paquetes para obtener información valiosa que se mueve sobre la red, un ejemplo de esto es hallar las contraseñas de los usuarios legítimos de la red cuando estos hacen uso de ella.

Algunas aplicaciones que usan para realizar esta función son Ettercap, desde ambiente Linux y Wireshark desde ambiente Linux o Windows

4.3.6 Piratas Informáticos. Son comparados con los crackers, pero a diferencia de estos realizan acciones ilegales buscando un beneficio propio, se dedican a la reproducción y comercialización y distribución ilegal de todo tipo de contenido digitales, afectando en gran medida la propiedad intelectual de los productores legítimos como cineastas o músicos.

4.3.7 Ingeniero Social. Estos son los que representan interés para el trabajo de monografía y en estos se enfocará el interés. Según Hadnagy (2010), los ingenieros sociales pueden adoptar varias características, pueden ser amigables o pueden dedicarse a destruir o crear[51] existen 10 formas distintas de ingenieros sociales que se pueden clasificar:

4.3.7.1 Hackers. Estos ya fueron clasificados, pero viendo los avances tecnológicos en la actualidad, un hacker puede ser un perfecto ingeniero social quien tiene como finalidad perfeccionar sus ataques que pueden ser dirigidos a usuarios comunes o a sectores de categoría pública o privada.

4.3.7.2 Espías. Son las personas que de forma encubierta logran obtener información valiosa para quien los contrato, este tipo de ingeniero social logra adoptar varios estilos de vida, asumiendo diferentes roles, logrando hacer creer su personaje y así poder obtener la información que busca.

4.3.7.3 Ladrones de identidad. Son los ingenieros sociales que logran robar la identidad y hacerse pasar por otra persona, ya sea de la esfera pública o privada

[51] HADNAGY, Christopher. Ingeniería Social. El Arte del Hacking Personal. Anaya multimedia.2010

con el fin de acceder a recursos o la obtención de beneficios a nombre de la persona legitima, hoy en día estas personas usan esta técnica en redes sociales para crear falsas cuentas y difamar a personas o levantar calumnias o de acuerdo a las intenciones que el criminal busque.

4.3.7.4 Estafadores. Son las personas que buscan cualquier oportunidad para hacer dinero, utilizan las necesidades de los demás para crear fachadas de organizaciones y proponer negocios rentables con ganancias jugosas y en el fondo no tiene ningún sustento legal, estos personajes son muy habitados y se escuchan a diario personas que fueron incautas por este tipo de personas[52].

4.5 TIPOS DE ATAQUES INFORMATICOS

4.4.1 Interrupción. Esto se logra cuando un servicio del sistema o red desiste de estar operativo y servible producto de una intrusión, es posible que el recurso del sistema quede no reutilizable en el peor de los casos. Un ejemplo se puede visualizar en la Figura 6.

Figura 6 Ataque por interrupción

Fuente: https://blogseguridadandrea.files.wordpress.com/2016/11/introduccion_seguridad_html_7f57ae53.png?w=300&h=227

En el ejemplo puede suceder que exista destrucción de hardware, un borrado total o parcial de los datos que no tengan respaldo, o fallos en sistemas operativos.

4.4.2 Modificación. Ataque por medio del cual se logra impactar la integridad de un sistema para modificarlo. Los ataques que llevan modificaciones de los sistemas

[52] GRAÑA, Lara. Alerta frente a las ciberestafas [En Línea]. 2016. [Citado 08-Noviembre-2018] Disponible en https://www.farodevigo.es/economia/2016/08/18/alerta-frente-ciberestafas/1517381.html

traen como consecuencias el detrimento total o parcial de los datos y los pueden dejar inutilizable. Este tipo de ataque es visible en la figura 7.

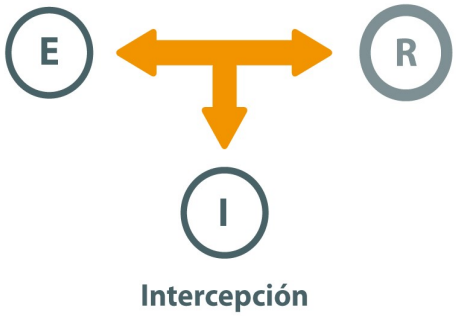
Figura 7 Ataque por modificación

Fuente: /elvira_mifsud/Introduccion_seguridad_html_m5e559c5b.png https://i1.wp.com/recursostic.educacion.es/observatorio/web/images/upload

La figura ilustra la modificación de la información, los sistemas atacados o pueden alterar los programas para que tengan un trabajo diferente, como crear puertas traseras.

4.4.3 Intercepción. Este tipo de ataque afecta la confidencialidad de un sistema ya sea por medio de un programa, una subrutina o un proceso, el ciberdelincuentes consigue tener acceso al sistema sin autorización legítima. Estos ataques son silencios y a la vez difíciles de detectar ya que no producen un ataque directo al sistema; ilustrado en la Figura 8.

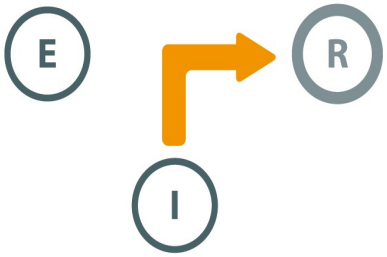
Figura 8 Ataque por interceptación



Fuente:
https://i1.wp.com/recursostic.educacion.es/observatorio/web/images/upload/elvira_mifsud/Introduccion_seguridad_html_m2554a7c.png

4.4.4 Fabricación. Este ataque crea peligro para la autenticidad de la información, y se logra cuando un atacante inserta objetos o subrutinas falsificados a un sistema como se puede observar en la Figura 9, esto puede darse con las direcciones IP, direccione WEB o correos electrónicos.

Figura 9 Ataque por fabricación



Fabricación

Fuente:
https://i2.wp.com/recursostic.educacion.es/observatorio/web/images/upload/elvira_mifsud/Introduccion_seguridad_html_24f07894.png

4.6 GENERALIDADES DE LA INSTITUCION

4.6.1 Misión. Formar ciudadanos y ciudadanas en los conocimientos, valores y competencias del saber administrativo público, para el desarrollo de la sociedad, el Estado y el fortalecimiento de la capacidad de gestión de las entidades y organizaciones prestadoras de servicio público, en los diferentes niveles de educación superior, educación para el trabajo y el desarrollo humano, la investigación y asistencia técnica en el ámbito territorial, nacional y global.

4.6.2 Visión. La ESAP en el 2019 será una institución de carácter universitario, de calidad académica acreditada, líder en la transformación de la sociedad, las entidades públicas y las organizaciones sociales. Órgano consultor del Estado en el saber administrativo público; difundiendo y generando conocimiento en los ámbitos nacional, territorial y global.

5 DISEÑO METODOLÓGICO

5.1 FASE 1 AUTORIZACIÓN Y ACUERDO DE CONFIDENCIALIDAD

Mediante la fase de autorización y acuerdo de confidencialidad se realizó un acuerdo entre la entidad educativa Escuela de administración Pública (ESAP) territorial Huila y los estudiantes Jasson Fabián Oliveros Ortiz y Reinaldo Enrique Ruiz. Para realizar la ejecución de la monografía titulada identificación de técnicas de ingeniería social ejecutadas en la entidad educativa Escuela Superior de Administración Pública, elaborando una autorización firmada por el coordinador administrativo y financiero. (Ver Anexo A).

5.2 FASE 2 APLICACIÓN DE ENCUESTA

Por medio de la realización de encuesta a todo el personal que labora en la Entidad Educativa de Administración Pública (ESAP) se buscara recolectar información aplicando unas preguntas cerradas (Ver anexo B), para ello se aprovechó las reuniones de área que tienen los docentes y administrativos de la Entidad, esta reunión se hace cada mes con el fin de retroalimentar los términos y objetivos propuestos por la organización, allí se solicita de la colaboración de los asistentes y se les explica la finalidad de la misma.

El cuestionario sobre la percepción de la seguridad informática en la escuela superior de administración pública ESAP contó con 10 preguntas relacionadas con la seguridad informática teniendo en cuenta la ingeniería social como contexto principal de la encuestas, se realizó a 70 funcionarios entre docentes y administrativos presente; en dicha reunión respondieran la encuesta satisfactoriamente, se explica cómo se debe responder las preguntas y se queda atento ante cualquier inquietud que tengan sobre la encuesta relacionada

5.3 FASE 3 RECOLECCIÓN DE LOS DATOS Y ANÁLISIS

Luego de recoger todas las encuestas se hace necesario organizar y tabularlas para poder realizar un análisis gráfico y de porcentaje sobre la información encuestada y así generar para la entidad unas conclusiones y recomendaciones que puedan ser aplicadas con el fin de aumentar y elevar la seguridad con temas relacionados con la Ingeniería social y sus métodos de aplicación.

Es importante que para este paso sean tenidos en cuenta las metodologías de un ataque por ingeniera social, que fueron descritas en el marco teórico, aquí se tendrá en cuenta los cuatros pasos incluidos y estos deberán ser mostrados a todos los

empleados por medio de capacitaciones para que sea de pleno conocimiento para cada uno de ellos y sea de fácil reconocimiento.

5.3.1 Selección y reconocimiento.

En este paso se explica a todos los empleados de la ESAP los métodos más usados para poder acceder a la información y así implementar un ataque por ingeniería social que sea efectivo, se buscará dar explicación de lo que es phishing y todos los métodos de ataques basados en la tecnología descritos en el trabajo, aquí se torna importante mostrar a los empleados de la ESAP los medios electrónicos más usados por los cuales es posible realizar un ataque por ingeniera social como son el correo electrónico, y a través de ellos los códigos maliciosos las características para determinar cuándo un correo es legítimo y cuando es de dudosa procedencia, identificar correos con mensajes de tipo spam.

También es importante mostrar a los funcionarios por medio de capacitaciones los tipos de atacantes que existen, qué papel tiene cada uno de ellos en la sociedad y así entrar a comparar e identificar que funciones pueden ejercer cada uno de ellos en el entorno de trabajo, haciendo profundidad en los ingenieros sociales.

Por otro lado, se deben recolectar en este nivel las encuestas realizadas en el ítem anterior para conocer de la mano el conocimiento previo que ahí sobre temas de seguridad en la ESAP y así poder tener una idea clara de estado de la infraestructura de la entidad.

5.3.2 Análisis y contacto

En esta fase se vuelve importante mostrar a los funcionarios de la entidad, las pruebas recolectadas y el nivel de información que logran obtener los ingenieros sociales sobre su víctima, al punto de conocer al detalle mucha información de su vida privada como de su ambiente laboral, que tipo de comidas son las preferidas, tipo de música que escucha, deporte favorito, horas en la que le gusta leer, los gusto en el cine y el arte, demás información que solamente sería importante para la víctima, pero el ingeniero aprende a distinguir cuando realiza sus ataques logrando recolectar valiosa información.

Con toda la información recolectada y el conocimiento de la víctima previo adquirido, es la parte donde los ingenieros sociales pasan a la segunda fase haciendo uso de toda esta información para tratar de entablar un vínculo con la víctima, donde se mostrara lo más amigable que pueden llegar a ser y poder hacerle creer a la víctima de lo importante de tener esas íntima amistad con el ingeniero social, crear una necesidad o dependencia con el ingeniero a fin de este lograr actuar y poder realizar

las fechorías para las que se propuso al momento de crear los vínculos afectivos con la victima

5.3.3 Generación del vector de ataque

Cuando ya se ha podido tener toda la información necesaria de la víctima y entablar el nivel de confianza optima sobre ella, es importante mostrar a los empleados el punto de manipulación que pueden tener los ingenieros sociales, a este nivel el ingeniero social, es capaz de intentar sobornar a la persona o empresa de la cual él obtuvo información sensible, como puede ser información de cuentas bancarias, credenciales de acceso de sitios de la empresa o información confidencial, con la finalidad de venderla a terceros o un pago por rescatar dicha información vulnerada.

Es muy importante mostrar a los funcionarios que cuando un ingeniero social se encuentra en esta fase tiene la capacidad de utilizar cualquier mecanismo que sea de fácil acceso para él, con tal de utilizar a su acomodo e interés la información obtenida y así, vulnerar a la víctima utilizando desde malware, keylogger, correos spam, obteniendo información y luego poder seguir con la última de las fases propuestas.

5.3.4 Ejecución de vector e intrusión

Habiendo aplicado las tres fases anteriores el ingeniero social ha podido cumplir con su objetivo, se podría decir que el ataque fue un éxito, en este punto logró comprometer información sensible de la víctima, cuentas de bancos e información que solo a la persona atacada le importaba, como ingresos a sistemas, a redes de comunicación a equipos con información de una empresa, redes sociales etc. En este punto de la aplicación de la metodología la conclusión para los funcionarios es que comprendan que cualquiera de ellos puede ser víctima de un ataque por un ingeniero social los cuales no distinguen estrato social ni condiciones económicas, es importante que los funcionarios creen conciencia sobre la información que manejan y el nivel de importancia que tiene por mi pequeña e insignificante que parezca.

5.4 FASE 4 DISEÑO DE LA INFRAESTRUCTURA TECNOLOGICA

Para el desarrollo de la infraestructura será necesario dentro del proceso de recolección de información, organizar la infraestructura existente teniendo en cuenta el inventario de los activos informáticos destacados de la escuela. Esta deberá ser de forma secuencial logrando acceder a las áreas físicas de la escuela siempre contando con el acompañamiento del personal del área de sistemas y tecnologías.

Organizado lo anterior, se procederá a realizar una comparación de los recursos actuales, con los que serán necesarios para proyectar una mejor seguridad sobre la entidad Pública ESAP, explicando el impacto que se puede lograr al utilizar esta infraestructura o nuevo modelo, se explica la forma en que los funcionarios se comunicarán entre sí y los mecanismos de seguridad que se podrán implementar para proteger de forma física y lógica los activos tecnológicos propuestos.

5.5 ACTIVIDADES PARA ATENUAR LA INGENIERÍA SOCIAL EN LA ENTIDAD

Con el fin de minimizar los ataques por medio de las técnicas implementadas para la ingeniería social, se toman medidas las cuales deben estar aplicadas en las políticas de seguridad de la entidad educativa. Para no convertirnos en víctimas de la ingeniería social hay tomar las siguientes precauciones:

5.4.1 Concientización. Todos los funcionarios de la empresa deben estar en la capacidad de reconocer cuando un ingeniero social está cerca y las intenciones que lleva, pero para identificarlo es importante tener ciclos de capacitación permanente con el personal de la organización, para conocer la metodología de ataque que se utiliza en la ingeniería social y las consecuencias que estas tienen sobre la empresa[53].

5.4.2 Correo. El uso de correos electrónicos es fundamental en las entidades, por este medio se comunican los clientes con proveedores y los mismos empleados. Diariamente llegan muchos mensajes al buzón de los correos, algunos de ellos son maliciosos con enlaces a páginas desconocidas o archivos adjuntos con malware. Para evitar este tipo de ataque se debe capacitar al personal con las siguientes instrucciones:

- Sospechar de cualquier correo que solicite información de manera urgente.
- Verificar la redacción de los correos, por lo general los sospechosos no contienen una buena redacción o contiene errores ortográficos.
- Verificar la ruta de los enlaces ya que pueden llevar a sitios desconocidos e ingresar virus al equipo.
- Tener actualizado el antivirus.
- Instalar las actualizaciones disponibles en el sistema operativo.

[53] QUEZADA, Alonso. Defensas Contra Ataques De Ingeniería Social [En Línea]. 2017. [Citado 15-Noviembre-2019] Disponible en: http://www.reydes.com/d/?q=Defensas_contra_Ataques_de_Ingenieria_Social

5.4.3 Llamadas. Hay que tener precaución porque mediante esta modalidad se sustrae información importante. Para prevenir este tipo de modalidad tengan en cuenta las siguientes recomendaciones; No dar información de usuarios y contraseñas, Desconfiar de llamadas con números desconocidos.

5.4.4 Backup's y copias de respaldo. Estos ayudan a que, aunque se perpetre un ataque y haya pérdida de información ayuden a restaurar el negocio a un punto de retorno y dar la normalidad a los procesos, hay que realizarlas de maneras periódicas y en lo posible almacenar en lugares diferentes de las instalaciones físicas[54].

[54] FUNDACIÓN UNIVERSITARIA CATÓLICA DEL NORTE. La importancia de los Backups [En Línea]. 2012. [Citado 18-noviembre-2018]. Disponible en : https://www.ucn.edu.co/cpe/r8/sala-prensa/Paginas/La-importancia-de-los-Backups.aspx

6 DISEÑO DE LA INFRAESTRUCTURA TECNOLÓGICA

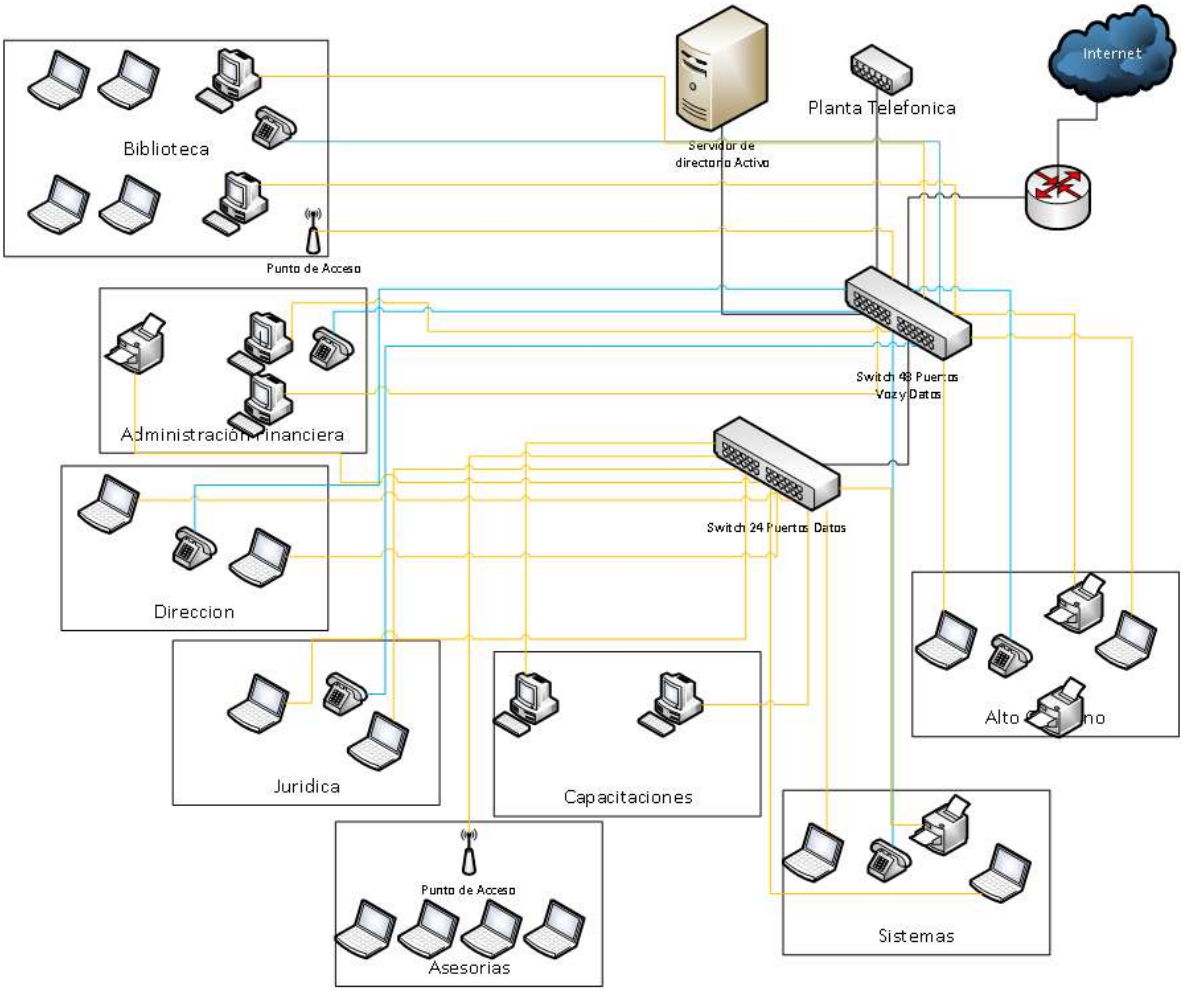
Para la realización del diseño de la infraestructura, se tendrá en cuenta inicialmente realizar un diagnóstico de la infraestructura actual de la institución pública ESAP, en ella se realizará el levantamiento de los activos informáticos que tiene la Escuela, organizando toda la información relacionada con el inventario de los equipos se procede a realizar un diagrama donde se podrá ver la arquitectura física que está montada y mostraremos de manera general como los datos son utilizados y como se maneja los implementos tecnológicos.

6.1 DIAGNOSTICO DE LA INFRAESTRUCTURA TECNOLÓGICA

El diagnostico a elaborar debe iniciar con el levantamiento de la información correspondiente a los activos tecnológicos que están presentes en la escuela. Para eso se realizará un inventario de todos los equipos que se utilizan por área, este inventario será realizado de forma secuencial teniendo en cuenta las dependencias, para esto se solicitó permisos para ingresar a la empresa y se consultó la información con el personal de informática y tecnología.

Luego de haber sido facilitada la información se organizará un diagrama de red de forma general de la infraestructura tecnológica con el fin de poder entender la interacción que tienen cada elemento dentro de la escuela. Se explica que no será necesario entrar en detalle de las interconexiones entre los elementos, simplemente se realizará una muestra de los procesos críticos y se realizará un diagrama de manera general para así comprender de una forma global la infraestructura que tiene la escuela.

Figura 10 Diagrama Actual de la Red ESAP



Fuente: Los Autores

En la figura 10 se puede identificar varios equipos de cómputos de tipo desktop “torre” y equipos portátiles; todos ellos conectados de forma equitativa a dos Switch; uno de 48 puertos que gestiona voz y datos y otro de 24 puertos. Al Switch de 48 se conectan toda la telefonía IP que viene de la planta telefónica, además de eso hay un área que es la que maneja un punto de acceso inalámbrico y en ella se conectan solamente una serie de equipos que es el área de biblioteca. También se puede identificar conectadas impresoras en varias dependencias de la Escuela, todos los equipos que trabajan en la escuela se encuentran funcionando bajo sistema operativo Windows 10, y el servidor tiene instalado un sistema operativo Windows Server 2016.

La Figura 10 presenta de manera general la información de activos informáticos de la ESAP basado en la información proporcionada por el INVENTARIO DE EQUIPOS TECNOLOGICOS E INFORMATICOS (ver Anexo C), del cual se logró realizar el

siguiente resumen de los principales componentes que tiene la escuela como se muestran en la tabla 1.

Tabla 1. Organización general de componentes tecnológicos

Información general de los componentes		
Elementos	**Cantidad**	**Observaciones**
Pc portátil (laptop)	150	Todos los equipos cuentan con Windows 10 Core i5 y Core i7
Impresoras	10	Son impresoras láser negras
Pc Torres (desktop)	40	Todos los equipos cuentas con Windows 10 Core i7
Servidor	1	Windows server 2016 Marca Dell
Software		
Windows 10	190	Licenciamiento Versión Pro en todos los equipos
Windows Server 2016	1	
Office 2013	190	Licenciamiento Standard para todos los equipos
AVG Internet Security	191	Software Pago
Canal de comunicación		
Claro	1	Cana de Datos de 20 Mbps
Telefonía		
Planta Telefónica	1	Capacidad para 2 líneas y 50 Extensiones
Teléfonos VoIP	20	Digitales administrados por la planta telefónica
Gestión		
Switch	2	24 y 48 puertos
Router	1	Acceso a Internet

Fuente: RUIZ DUARTE, Reinaldo; OLIVEROS ORTIZ, Jasson. Diagnóstico de la infraestructura tecnológica

Es importante anotar que con el esquema propuesto se hace un análisis general de lo que es el diagrama de la red, para este caso no se tiene en cuenta los detalles de la configuración y las características particulares, todos estos elementos

utilizados en las tablas son propios de la entidad pública ESAP, lo que genera independencia sobre ellos.

Con el esquema anterior se podrá concluir que la infraestructura no es suficiente para que la ESAP pueda garantizar una plataforma segura de comunicaciones, así como garantizar a sus trabajadores áreas donde logren acceder a los equipos sin el riesgo de que puedan ser víctimas de ataques sea por ingeniería social u otro tipo de ataques más técnicos como por ejemplo la técnica de XXS Cross Site, SQL injection entre otros. Tampoco se evidencia una plataforma segura para la navegación por el internet, se identifica que la información se está manejando de una forma centralizada pero el servidor está muy expuesto a cualquier tipo de ataques informáticos como la interrupción, modificación, intercepción y fabricación,

También se observa como la empresa en aras de resguardar la red, ha tomado conciencia en temas de la seguridad con la adquisición de software como antivirus privativo utilizándolo en todos los equipos. El antivirus puede ofrecer resultados positivos de protección sobre la red, pero se considera que este es el paso inicial para crear un mecanismo que pueda ayudar a brindar un esquema de seguridad eficaz.

6.2 DISEÑO DE UNA INFRAESTRUCTURA TECNOLÓGICA

Para realizar el diseño óptimo de una infraestructura tecnológica, se hace necesario referenciar los elementos a tener en cuenta en una arquitectura de red. Estos serán comparados con el modelo existente en la escuela con el fin de determinar el nivel de implementación que se encuentra el diagrama con el fin de adquirirlos y actualizarlos.

También se realizará un proceso comparación entre el estado actual de la tecnología que utiliza la escuela con relación a la utilizada en otro tipo de empresas que están a la vanguardia en plataformas tecnológicas aplicadas en las empresas en el mundo moderno, luego se realizará un diseño en donde se reúna los requerimientos para brindar una seguridad a la infraestructura tecnológica y soporte una implementación de medidas de seguridad para la institución educativa ESAP.

6.2.1 Verificación de los recursos tecnológicos

Teniendo claro los equipos de una forma general que están instalados en la institución, es importante realizar un comparativo con los equipos necesarios con el fin de tener una idea del presupuesto necesario a tener en cuenta para poder dar una correcta implementación de plan de mejoramiento de la red y la seguridad

dentro de los activos de la entidad, garantizando seguridad con respecto a ataques por ingeniería social como se describe en la tabla 2.

Tabla 2. Comparación de elementos tecnológicos necesarios

	Mínimo necesario	Actual	Análisis
HARDWARE	UPS	No existe	Para garantizar una seguridad mínima sobre ataques generados por ingeniería social son necesarios los siguientes elementos, se observan que el 100% de los elementos actuales pueden ser aprovechado|
	Firewall	No existe	
	Rack	Existen	
	Patch Panel	Existen	
	Equipos computo	Existen	
	Teléfonos	Existen	
	Scanner	Existen	
	Planta telefónica	Existen	
	Impresoras	Existen	
	IDS/IPS	No existe	
	Servidor Backups	No existe	
SOFTWARE	Internet	Existe	Se cuenta con sistemas operativos licenciados y actualizados, así como antivirus de tipo licenciado, pero no se está dando protección a los datos que llegas a las bases de datos del servidor
	Software Firewall	No Existe	
	Base de datos		
	Sistemas Operativos Recientes Windows 10	Existen	
	Antivirus	Existen	
	Ofimática	Existen	
	Software Backup	No Existe	

Fuente: RUIZ DUARTE, Reinaldo; OLIVEROS ORTIZ, Jasson. Verificación de los recursos tecnológicos

Al examinar la tabla 2 se distinguen aspectos importantes a tener en cuenta en el diseño de una implementación segura contra ataques en la escuela superior administración pública ESAP. Se puede identificar que la escuela no cuenta con equipos de seguridad de tráfico de datos, tampoco se evidencia equipos que se encarguen de realizar filtrados de puertos y garantizar la navegación segura, así como tampoco un software que ayude a proteger las bases de datos internas que tiene la ESAP.

Por otro lado, se evidencia que la mayoría de la información que manejan, es almacenada de forma local en los equipos y no se está llevando un Backup que respalde la información ante un siniestro de robo o pérdida de estos. Toda la información que sale de la empresa, se realiza por medios electrónico ya sea por email o discos extraíbles, que son utilizados por los empleados para cumplir las demandas diarias de información que surgen en la escuela. No se está llevando

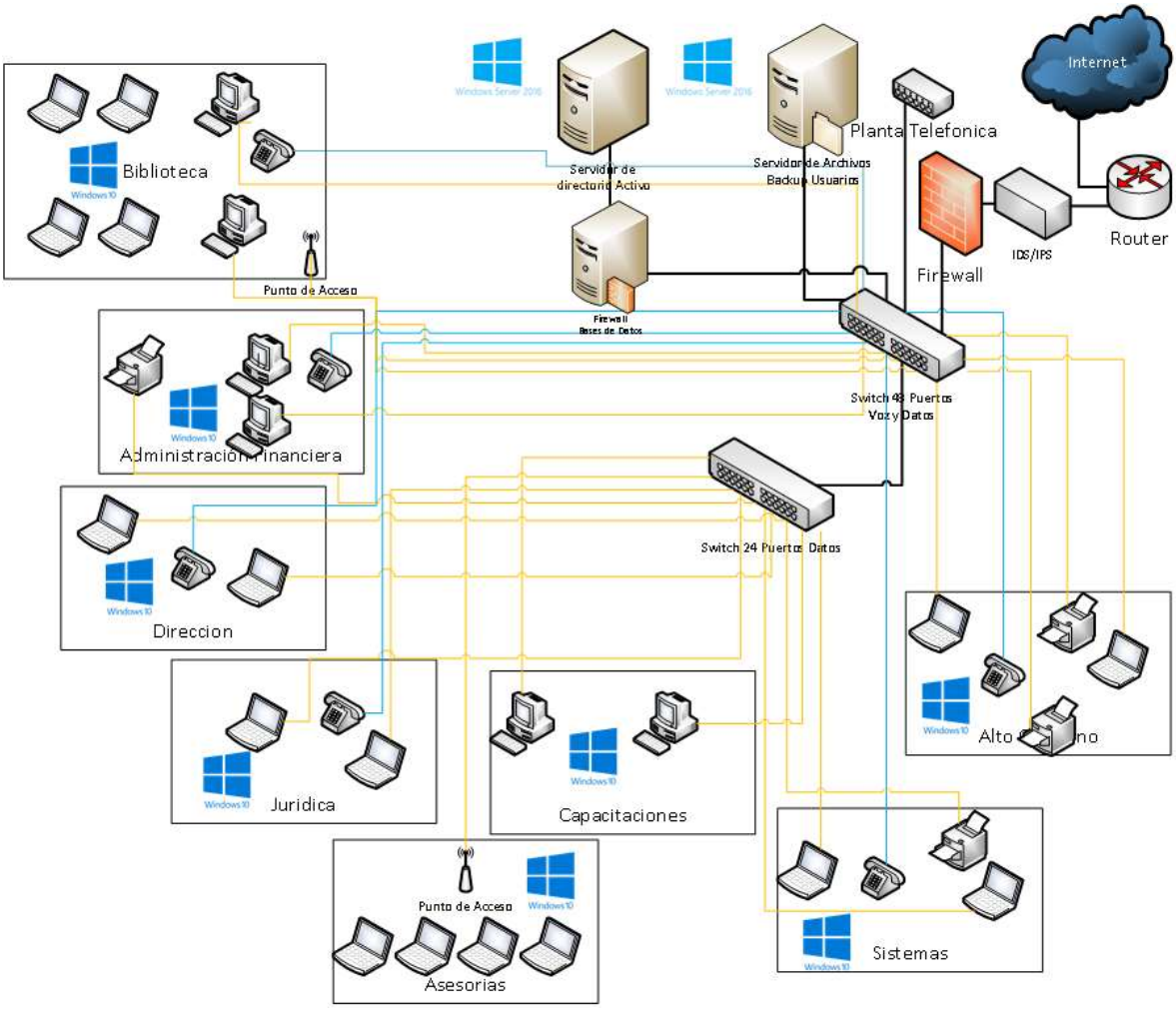
filtros de navegación en internet, aspecto importante a tener en cuenta, sabiendo que es el medio de comunicación principal de la institución, tampoco se observa algún dispositivo que respalde en caso de ausencia de energía, lo que supone un riesgo mayor en la ESAP al momento que haya ausencia de esta.

6.2.2 Diseño de infraestructura tecnológica segura

Después de poder observar y realizar un análisis profundo de la infraestructura tecnológica actual de la institución, se procede a realizar un diseño con los recursos necesarios, para garantizar la implementación el análisis anterior. Lo recomendado es tratar de reutilizar, todos los elementos que tiene la escuela actualmente con el fin de reducir los costos que generen la implementación y garantizar la operatividad entre todos los dispositivos presentes en la red.

Lo recomendable es diseñar una topología basada en la infraestructura tecnológica tipo estrella, aprovechando sus ventajas y cualidades, teniendo presente las recomendaciones de continuidad eléctrica y todos los temas relacionados con la red LAN, su custodia y aseguramiento, es importante decir que los dispositivos que se encuentren interconectados deban tener la mayor integridad y homogeneidad posible, brindando una simple y segura comunicación entre todas las partes y la interconexión segura entre los equipos.

Figura 11 Diagrama propuesto de la Red ESAP



Fuente: Los Autores

En la figura 11 se puede observar de forma general como quedaría conformada la infraestructura propuesta, es de aclarar que se reutiliza el 100% de los elementos antes encontrados en la revisión inicial aparte se han incluidos los elementos mínimos necesarios para la infraestructura de la escuela, con el fin de brindar seguridad evitando ataques de ingeniera social por software y así cubrir las necesidades que ellos desean cubrir

Con la implementación de los dispositivos como son el firewall de bases de datos, firewall como controlador de tráfico a nivel general de la red de la empresa y un IDS para ayudar a proporcionar conexiones, recepción y envío de paquetes de manera segura se busca es ayudar a proporcionar una seguridad más integral sobre el diagrama de la red ya que nos percatamos que en la topología original que

presenta la empresa demostrado en la figura10 no hacen uso de estos recursos tecnológicos que ayudan a controvertir otras formas de ataques utilizados por los hacker y que como profesionales de la seguridad que somos no deberíamos pasar por alto estos dispositivos que existen en el mercado y ayudan a reducir los riesgos mejorando las posturas de seguridad en las organizaciones.

Con este diseño, se plantea realizar la instalación de un firewall físico de la línea Sophos XG equipos que ayudarán con la seguridad del tráfico de paquetes en la red apoyado con las políticas ya existentes; tendrá como finalidad la de monitorear el tráfico de paquetes de la red después de la señal que viene del router y avisar cuando se presenten eventos de posibles intrusiones maliciosas, además se habilita un firewall físico que ayudará a bloquear acceso a sitios no seguros para los funcionarios de la escuela.

Por otro lado, también se informa a las directivas sobre cuáles son las mejores formas de aplicar seguridad al acceso del antiguo servidor del directorio activo que opera las bases de datos actuales, implementando un firewall exclusivo para estas con el fin de llevar filtros con reglas preestablecidas, y así dar control a las peticiones que llegan a los motores de bases de datos, bloqueando las peticiones maliciosas y llevando el control monitorizado de todas las actividades que se gestionen sobre el servidor.

6.2.2.1 Configuración de los dispositivos de seguridad:

6.2.2.1.1 Firewall:

Es el Hardware que protege la red de las posibles instrucciones de las redes externas a la ESAP; Mediante el sistema de filtros de paquete de datos custodia la información que circula en la red local y la red externa. Es el intermediario entre las rede local de la ESAP y la Red externa por ende no permite que circulen paquetes de datos o salgan de la red, si no están en la lista permitida por el firewall.

Se ejecutan las siguientes reglas:

- Autorizar una conexión (Allow)
- Bloquear una conexión (Deny)
- Redireccionar un pedido de conexión sin avisar al emisor (Drop).

Mediante las reglas de Allow, Deny y Drop, se establece la política de seguridad:

Permitir solamente lo que esté autorizado; si no está autorizado es prohibido y debe ser bloqueado. El filtrado se controla en la capa OSI 3 (red) y 4 (transporte) donde se controla al tomar el encabezado de protocolo cada paquete de datos. Es importante recalcar que se implementa la identificación de direcciones MAC para un mejor control.

6.2.2.1.1.1 Reglas a implementar en la configuración del firewall para la protección de la red de la ESAP:

Se administra el acceso al servidor: Solo puede ingresar a los aplicativos del servidor y sus funciones, los usuarios autorizados por el área de sistemas, solo tendrán permisos de administrador los usuarios que por su perfil profesional necesiten acceder a los aplicativos según las funciones asignadas.

Monitorear y registrar todos los accesos de entrada y salida de la red de la escuela superior de administración pública, este proceso se almacena en logs, con la finalidad de ser procesado por el área de sistemas encabezado por el ingeniero encargado de la seguridad informática.

Control al acceso a internet de las aplicaciones, con la finalidad de proteger la información se restringe el uso de internet de las aplicaciones que no están autorizada para el funcionamiento de la ESAP.

Aplicar el filtro de protocolo, se utiliza con la finalidad de filtrar el tráfico de la red según el protocolo permitido.

Dirección donde se agregarán las reglas:

“/ip firewall filter"

Dejar pasar todo el tráfico de internet hacia la LAN

“add action=accept chain=input comment="" disabled=no dst-port=8291 in-interface=pppoe-out1 protocol=tcp”

Pasar todas las conexiones establecidas hacia la red publica

“add action=accept chain=input comment="" connection-state=established disabled=no in-interface=pppoe-out1”

Permisos a aplicaciones para tráfico (se hace por aplicación utilizada)

add action=accept chain=input comment="" connection-state=related disabled=no in-interface=pppoe-out1

Se Cierra todo el tráfico adicional para que por WAN o LAN lo descarte el firewall

add action=drop chain=input comment="" disabled=no in-interface=pppoe-out1

6.2.2.1.2 IDS

Para la IDS o sistema de detección de intrusos haremos uso de una herramienta robusta como lo es Snort con la aplicación de reglas basadas en el modelo de usos indebidos, esto con el fin de proceder a reconocer ataques y firmas de intrusión, estas reglas serán agrupadas en conjuntos de firmas donde serán categorizados los incidentes y así encontraremos detección de troyanos, keylogger, detección de ataques de tipo buffer, overflows, entre otras. Que apoyarían la detección temprana de alertas en caso de uso de ingeniería social sobre la Entidad.

6.2.2.1.2.1 Reglas a implementar en la configuración del IDS para la protección de la red de la ESAP:

Para ello dentro de la herramienta Snort crearemos un fichero de reglas nuevo (.rules) dentro del directorio rules y luego editamos el fichero de configuración de Snort con las siguientes reglas.

- Regla Acceso anónimo FTP: alert tcp $EXTERNAL_NET any -> $HOME_NET 21 \(msg:”UOC – Anonymous FTP Access”; \content:”USER anonymous”; \classtype:suspicious-login; sid:99999901; rev:1;)
- Regla Exploit exploit/unix/ftp/vsftpd_234_backdoor: alert tcp $EXTERNAL_NET any -> $HOME_NET 21 \(msg:”UOC – Exploit VSFTPD v.2.3.4 Backdoor Command Execute”; \content:”USER”; content:”:)”; \classtype:suspicious-login; sid:99999902; rev:1;)
- Regla Exploit exploit/multi/samba/usermap_script: alert tcp $EXTERNAL_NET any -> $HOME_NET 139 \(msg:”UOC – Exploit Samba ‘username map script’ Command Execution”; \content:”|2f 3d 60 6e 6f 68 75 70 20|”; \classtype:string-detect; sid:99999903; rev:1; reference:cve,2007-2447;)
- Regla Exploit exploit/multi/misc/java_rmi_server: alert tcp $HOME_NET any -> $EXTERNAL_NET 8080 \(msg:”UOC – Exploit Java RMI Server Insecure Configuration Java CodeExecution”; \uricontent:”.jar”; content:”GET”; http_method; \pcre:”/\/(\w|\d)+\/(\w|\d)+\.jar/i”; \classtype:suspicious-filename-detect; sid:99999904; rev:1;)
- Regla Exploit exploit/linux/misc/drb_remote_codeexec alert tcp $EXTERNAL_NET any -> $HOME _NET 8787 \(msg:”UOC – Exploit Distributed Ruby Send instance_eval/syscall CodeExecution”; \content:”syscall”; \content:”#!/bin/sh”; content:”sh -c”; \classtype:string-detect; sid:99999909; rev:1;)

6.2.2.1.3 Keylogger:

Es un software que tiene la capacidad de obtener la información que se teclea sin que el usuario se dé cuenta; este tipo de ataque puede guardar la información obtenida localmente en el pc o en su defecto enviarlo a otro pc, según sea la instrucción del atacante. La forma de instalarse este software es por medio de un malware cuando el usuario descarga e instala una aplicación de una página desconocida o ingresa a un link sin conocer la procedencia.

6.2.2.1.3.1 Implementación de políticas de seguridad para protegerse de un keylogger:

- Mantener el antivirus actualizado
- Realizar cambio de contraseña mensual, bajo la petición del servidor.
- Los usuarios no tienen permisos de administrador sobre el pc, los privilegios son limitados.
- Dar control de permisos administrativos sobre usuarios estándares, desde el directorio activo de la entidad con el fin de dar restricciones a los usuarios sobre el acceso a recursos tecnológicos, y la utilización de las estaciones de trabajo.
- Habilitar la autenticación de 2 factores, con la finalidad de proteger la cuenta incluso si ha descifrado la contraseña.
- Limitar el acceso a páginas sospechosas habilitando las listas negras en las políticas de Firewall

7 RESULTADOS Y EVIDENCIAS

Para proporcionar el bosquejo inicial sobre la temática que se está trabajando, se propuso realizar una encuesta con preguntas tipo cerrada y única respuesta (Ver anexo C) para ello se aprovechó las reuniones de área que se hacen con todo el personal administrativo y docente que laboran en la institución, solicitando cordialmente la colaboración para que la diligenciaran.

Se logró aplicar la encuesta a 70 asistentes quienes respondieron satisfactoriamente, se incluyó personal de todas las dependencias de la institución, se excluyó a personal que trabaja con la escuela pero que pertenecen a otras sedes de la organización, solamente se incluyó al personal que trabaja tiempo completo en la sede en Huila.

Los resultados entregados a continuación son en mayor parte producto de un análisis exhaustivo realizando preguntas enfocadas con el desarrollo de los objetivos planteados por esta monografía para recolectar datos, se diligenciaron las 70 respuestas es un formulario diseñado en Excel desde el cual se implementó la herramienta de tablas dinámicas con el fin de utilizar los diferentes gráficos para entender de una manera adecuada los resultados encontrados. La encuesta se realizó a todos los funcionarios que tienen acceso a los equipos e información de la institución.

7.1 CASO PRÁCTICO

Para poder desarrollar y entender el peligro que representa el ataque de ingeniería social a nivel general, se realizó la ejemplificación de cómo piensa y actúa un cibercriminal, con un paso a paso de lo que puede ser una ataque por ingeniería social en las instalaciones de la Escuela Superior de Administración Publica ESAP, con el único objetivo de demostrar que un ataque de esta magnitud es posible y fácil para una persona que tenga el conocimiento y los medios necesarios, aprovechando la vulnerabilidad que se encuentran actualmente en las sedes tanto a nivel tecnológico como a nivel de talento humano.

Al realizar el ataque por ingeniería social a la ESAP fue necesario un software cuya herramienta denominada “Social-Enginneering Toolkit” es distribuida por Kali Linux con este software se realizó un ataque tecnológico avanzado por ingeniera social y de forma automática se generó una serie de ataques con el que se comprometió el recurso humano de la escuela.

Dividiendo el ataque en 4 pasos importantes:

7.1.1 Identificación de la victima

Este paso se aplicó sobre todo el personal humano que labora en la sede y está conectado a los equipos o recursos tecnológicos de la institución, ya fueran los corporativos, propios, conectados al email, o con acceso a portales y/o cualquiera de los servicios de la web de la escuela superior de administración pública.

7.1.2 Reconocimiento

Al indagar la seguridad que se encuentra en la sede, y utilizando el perfil de funcionario de la entidad, se buscaron puntos de red asequibles y activos, con el fin de encontrar en primera medida el rango de direccionamiento IP con el que están trabajando en la escuela; además, se ubicó de forma precisa las oficinas de informática, así como los equipos que tienen fácil acceso para usuarios y así poder encontrar que tan segmentada estaba la red. Se realizaron múltiples pruebas básicas dentro de las que se deberá tener conexión a redes inalámbricas en puntos visibles de internet, utilizando la Ethernet que se encuentra activa en las instalaciones.

Se opta por realizar el ataque desde el área de la biblioteca, debido a que en esta se encuentran ubicadas las dos redes de la institución, existen usuarios invitados para brindar acceso a cualquier persona y además equipos administrativos con el que se da gestión y control de los usuarios que acceden a la sala. En este punto podemos concluir, que internamente la red se encuentra segmentada en 2 VLAN y que estos conectan al mismo servidor.

7.1.3 Creación del Escenario

Para la creación del escenario, fue necesario realizar la suplantación del correo institucional, y cuando un usuario legítimo intentara tener acceso a dicho correo este fuese logueado por el falso servidor de correo, todo esto se realiza con el fin de obtener información confidencial que maneja el usuario y que caiga fácilmente en la trampa que se preparó para él, la tarea puede demorar varios días en los cuales se capturara y almacena toda la información necesaria para hacer que alguno de los funcionarios caiga en el engaño.

7.1.4 Realizar el ataque

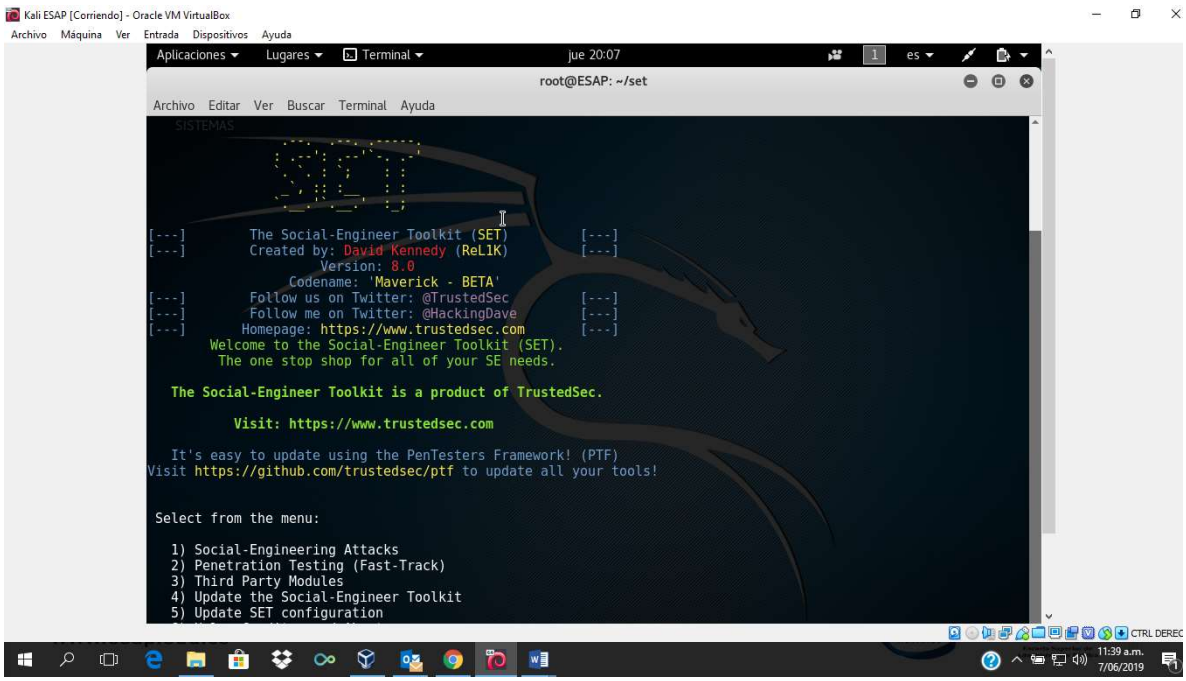
Logrando el acceso físico a las instalaciones de la institución, teniendo a la mano los equipos necesarios y la herramienta lista, se procedió a realizar el ataque por

ingeniera social, utilizando la herramienta The Social Engineering Toolkit (SET) integrada en la distribución Kali Linux, es de aclarar que la prueba se realizó en un ambiente controlado, con la finalidad de identificar la vulnerabilidad que existía en la ESAP y los podría convertir en víctimas de ataques por ingeniería social.

Fue necesario iniciar con la presentación de las imágenes, con las cuales se describió el proceso que fue realizado para obtener la información, recordándoles que este tipo de herramientas, solamente funciona dentro de áreas de red local y que es sumamente importante mantenerla actualizada para su funcionamiento, haciendo uso de las herramientas que tiene disponible las distribuidoras como lo es Kali Linux.

Cuando se estaba dentro de la aplicación se visualizaba el siguiente pantallazo, ilustrado en la figura 12, en este se pudo evidenciar el ambiente de trabajo que ofrece la herramienta, desplegó un menú de opciones y para la realización de la prueba se seleccionó la opción 1 que enuncia “Social-Engineering Attacks”.

Figura 12 Presentación Del SET "Social-Engineering Toolkit"

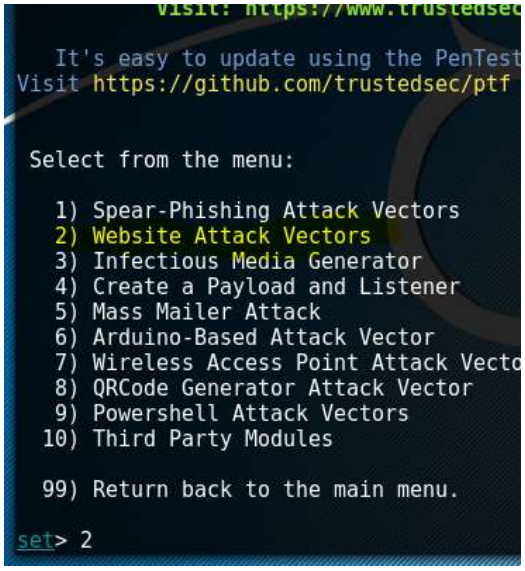


Fuente: Los Autores

Después de seleccionar la opción 1 “Social-Engineering Attack”, la misma herramienta pasa a la siguiente parte del menú y ofrece otras opciones en la que se elige el tipo de ataque que será aplicado sobre la red, para el caso realizado era la opción 2 “Website Attack Vectors” ilustrado en la figura 13, esta opción fue necesaria

seleccionarla porque es la que realiza la clonación del sitio web a atacar y hace creer al usuario final que el sitio web que está visitando es un sitio legítimo, aunque realmente estará entrando a un servicio web creado por la herramienta, que capturará sus datos personales.

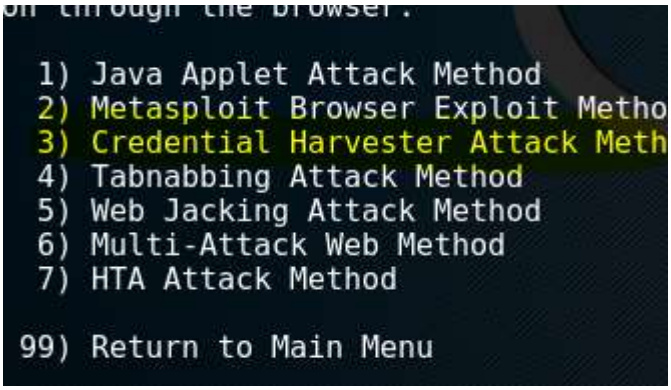
Figura 13 Selección de opción 2 "Website Attack Vectors"



Fuente: Los Autores

Se utilizó el ataque Credential Harvester Attack Method con el cual se clonó un sitio web y se subió al servidor de la máquina como se observa en la figura 14. La finalidad de utilizar este tipo de ataque fue poder obtener las credenciales de la víctima, en el caso aplicado, usuario y contraseña del correo institucional.

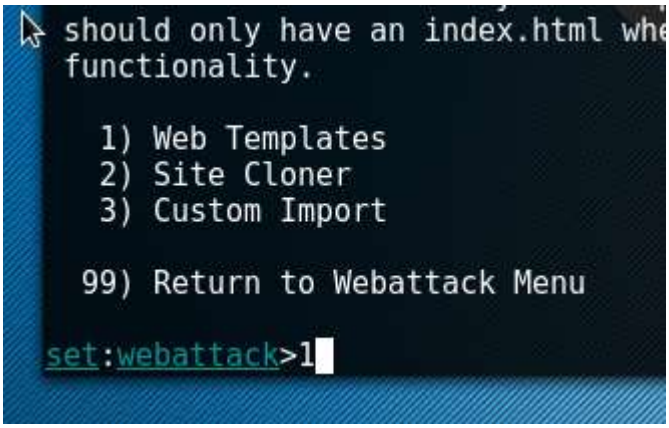
Figura 14 Selección de opción 3 "Credential harvester Attack method"



Fuente: Los Autores

Para el siguiente paso, ilustrado en la figura 15, era necesario utilizar la opción que dice “Web Templates” en la opción 1, con la cual se crearía la plantilla de la página web con la que se realizaría el ataque, pues esta modalidad facilita al ciberdelicuente poder obtener las credenciales mediante planillas predeterminadas de sitios web a utilizar.

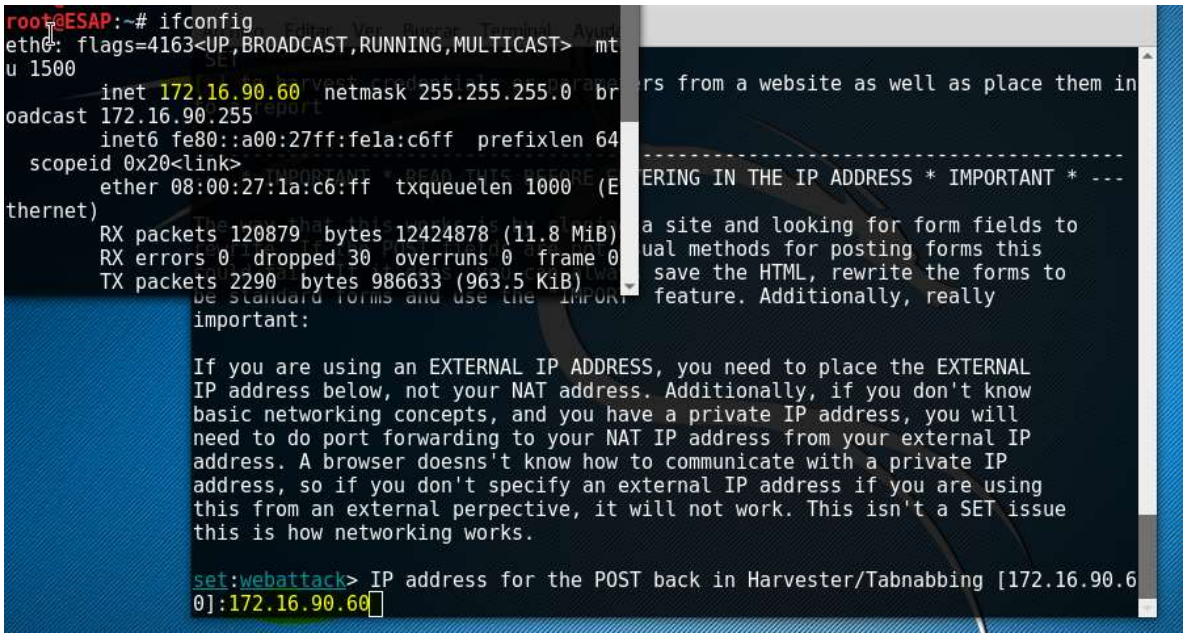
Figura 15 Selección de opción 1 "Web Templates"



Fuente: Los Autores

Seguidamente la herramienta solicitó el IP de la maquina atacante, se utilizó IP 172.16.90.60 Para obtener la dirección IP es necesario utilizar el comando ifconfig en la consola como se evidencia en la figura 16, seguido se utiliza la opción harvester/tabnabbing la cual recibe los datos de la víctima.

Figura 16 Selección de opción 1 "harvester/tabnabbing"



Fuente: Los Autores

Luego se selecciona la opción 2 “Google” la cual hace uso de la plantilla de google, esta plantilla viene predeterminada en la herramienta.

Figura 17 Selección de opción 1 "Google"

Fuente: Los Autores

Hasta este punto del desarrollo, ya se tenía configurada la plataforma para realizar el ataque, el paso a seguir fue enviar un correo masivo a los funcionarios de la empresa tomándolos del directorio corporativo de la entidad, esto se realizó haciendo uso de una cuenta falsa muy parecida a la que suministra el área de informática para darle un toque de credibilidad al asunto, este correo masivo era necesario para divulgar la información, lo que restaba era esperar que alguno de los usuarios cayera en la trampa, seleccionando el link que se había creado de acuerdo

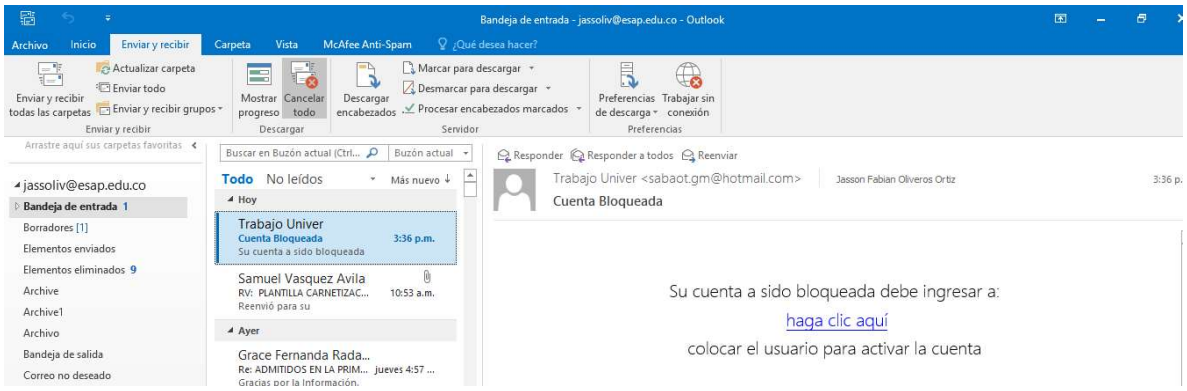
a la imagen y este fuese direccionado a la IP 172.16.90.60 mediante un mensaje en el enlace para poder capturar sus credenciales

Figura 18 Envío de correo falso

Fuente: Los Autores

Evidencia del correo spam recibido por la víctima ilustrado en la figura 18, es importante conocer un poco de la víctima y su necesidad para que pueda caer en el ataque, en este caso se informa al usuario que la cuenta está bloqueada y para poder acceder nuevamente a esta, debe ingresar al link que contiene la dirección falsa.

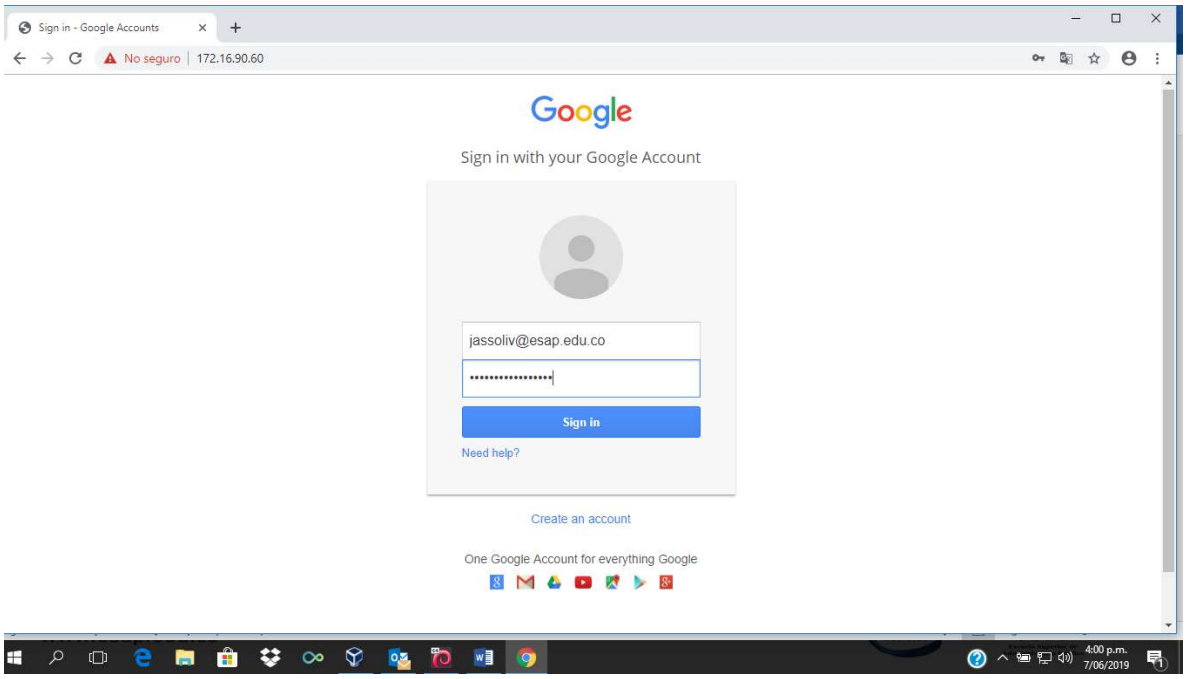
Figura 19 Evidencia de correo SPAM



Fuente: Los Autores

Cuando el funcionario dio clic sobre el link que se había enviado en el correo masivo, página muy similar al que proporciona en este caso los servidores de correo de google cuyo enlace fue el siguiente https://172.16.90.60 que correspondía a la dirección de la maquina atacante, esta intentaría realizar un login valido, como se evidencia en la figura 20

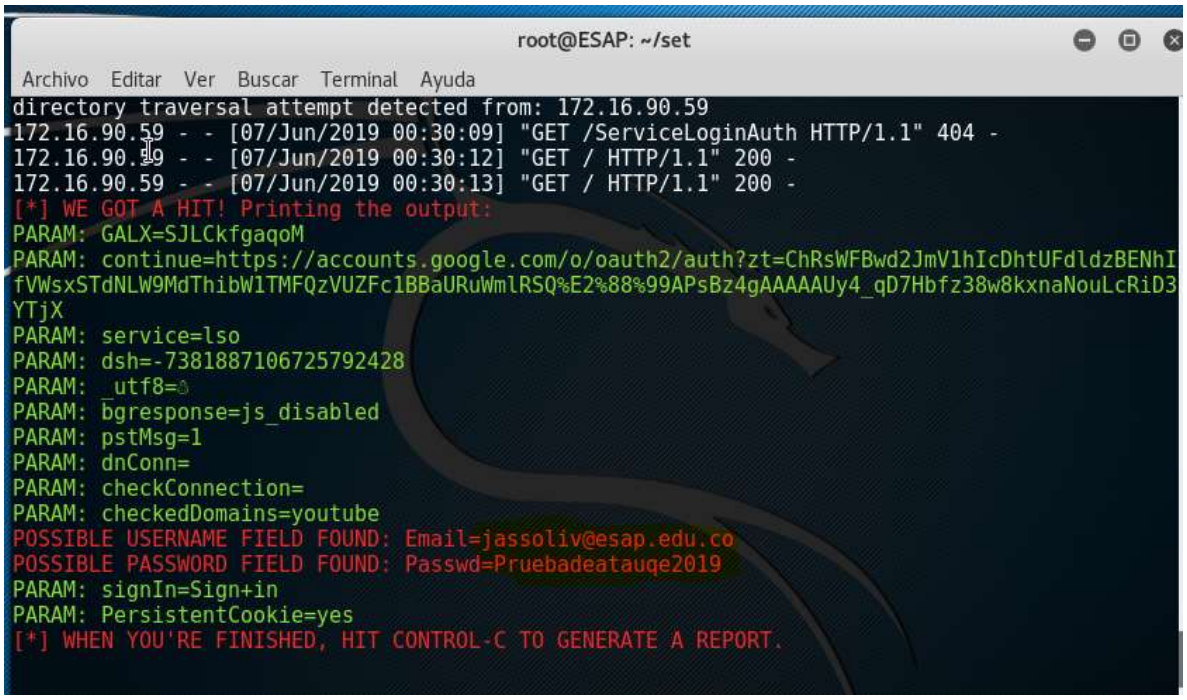
Figura 20 Página falsa creada para capturar credenciales



Fuente: Los Autores

En la máquina virtual atacante se evidenciará según la figura 21, cómo la víctima envío las credenciales al sitio web que se falsifico, el SET envía la dirección del correo electrónico y la clave correspondiente que ingresó el usuario víctima confirmando así, la efectividad del método utilizado en el ataque de ingeniería social.

Figura 21 Obtención de las credenciales



Fuente: Los Autores

Con la demostración del ataque realizado a la ESAP, y como se logra evidenciar, cualquier persona está expuesta, si no tiene un conocimiento básico para identificar los ataques y así evitar que este tipo de ciber crimen ocurra.

Luego de realizado el ataque, la persona encargada de perpetrar el crimen pudo fácilmente detener los servicios, apagar el equipo y salir de las instalaciones sin lograr despertar ningún tipo de sospecha del acto realizado, esto se debió a que en ningún momento los equipos de la red corporativa fueron vulnerados ya que todas las transacciones realizadas fueron legítimas, se envió un correo a un usuario legítimo, este accedió a un servicio que se encontraba dentro de la red LAN sobre el equipo atacante y se entregó información sin atacar los servicio de la empresa.

8 RECOMENDACIONES

La Escuela Superior de Administración Pública ESAP territorial Huila, debe realizar capacitaciones sobre temas de seguridad informática a todos los empleados sin hacer distinción alguna, el objetivo brindarle a cada funcionario las herramientas necesarias para que aprenda a proteger su información y los de la institución. Las capacitaciones deberán ser realizadas periódicamente en intervalos mínimos de un mes, se recomienda que sea dirigida por el personal encargado del departamento de Informática y tecnología.

Implementar la identificación biométrica u otro tipo de identificación electrónica, como las tarjetas con bandas electrónicas en los carnet de los empleados, así mismo implementarlo en las puertas de acceso a sitios restringidos al público porque es solamente para personal autorizado o contrato por la entidad, en lo posible si la entidad no dispone de recursos para la instalación de estos componentes electrónicos, se debe presionar al servicio de vigilancia para ejercer mayor control de las personas al ingresar a la entidad.

Así mismo es necesario la implementación de cámaras de seguridad en la entidad en todas las áreas o puntos donde se concentren la mayor cantidad de personas, para tener control visual de los activos informáticos de la escuela, así como del personal que los utiliza a diario

Toda la información que se encuentre en documentos en la entidad, que vaya hacer reciclada deberá ser triturada por maquinas hechas para tal fin, recomendando la adquisición de unos dispositivos de estos evitando así a que los ingenieros sociales por medio de la técnica Dumpster Diving obtenga información valiosa.

Realizar seguimientos periódicos a las bases de datos de antivirus, para verificar que se encuentren actualizadas o en su defecto migrar en busca de soluciones de antivirus orientadas en la nube con el fin de estar actualizando las terminales remotamente, así como llevar control de las amenazas encontradas en ellos y hacer gestión a la distancia.

Aplicar segmentación a las redes para utilización del WiFi, una para los empleados de la entidad, otra para los invitados y así evitar que la información de uso exclusivo de la Escuela sea accedida por invitados a la red, además se realizaría control de datos evitando saturación de los canales de internet contratados, por ende, se debe implementar actualización de dispositivos inalámbricos y segmentación de redes internas.

Se tendrá que administrar las cuentas de los usuarios de una forma centralizada, se hace necesaria la utilización de un directorio activo para llevar control de los usuarios que acceden a la información.

Es importante brindarles seguridad a los puntos de red del cableado estructurado, habilitando solamente los que son para el acceso del personal de la Escuela y deshabilitar los que no estén uso.

Incluir dentro de las políticas de seguridad, la restricción de redes sociales además del uso restringido de los servicios web, esto ayuda a fortalecer las medidas de seguridad y así mismo a mejorar la productividad de los empleados de la entidad.

Implementar dentro de las políticas de seguridad, restricciones para compartir archivos entre equipos en la misma red, solamente serán enviados archivos por email, previa revisión de los antivirus de los activos informáticos, en lo necesario si se necesita enviar algún documento utilizando medios extraíbles es necesario llevar una autorización previa de su jefe a cargo.

Realizar bloqueo de puertos USB de las terminales usadas por los empleados de la Escuela, evitando que cualquier persona pueda activar dispositivos sobre ellos y estos puedan descargar códigos maliciosos sobre los equipos y logren infectar las redes.

Realizar copias de seguridad de forma regular y periódica a los equipos y servidores de la Escuela, esto se puede implementar haciendo sitios seguros dentro de los equipos, como carpetas en las cuales faciliten esta labor de copias de seguridad y concientizar al personal de usar los equipos corporativos para uso exclusivo de labores de la Escuela.

Realizar mantenimiento periódico preventivo de los equipos de cómputos y/o servidores de la escuela esto con el fin de preparar los equipos y alargar su vida útil evitando en gran medida daños sobre ellos producto de mugre y suciedad que van adquiriendo en el tiempo.

9 CONCLUSIONES

Durante el trabajo realizado, se recopilaron todas las técnicas que actualmente se utilizan para realizar ingeniería social, de una manera resumida y fácil de entender, se explicaron los conceptos de cada una de ellas, buscando que el lector pueda entender el concepto y relacionarlo con algunos sucesos de su vida diaria, así mismo que aprenda a identificar las técnicas y cuáles son los métodos que se pueden utilizar en la ESAP; con la aplicación del simulacro de ataque a la escuela se logró describir las técnicas más usadas por los ingenieros sociales, demostrando lo fácil que fue realizarlo y salir sin algún problema, además se identificó que la entidad no cuenta con sistemas de control de acceso básicos, pues existen áreas a las cuales se logra acceder de manera fácil, sin que nadie ejerza control sobre las personas; así mismo los equipos ubicados dentro de áreas sensibles como es la administrativa, permite fácilmente el control de ellos con permisos administrativos y permitiendo realizar un ataque a gran escala dentro de la ESAP.

La red de la empresa principalmente la cableada tiene presente múltiples puertos de red habilitados que dan al acceso al público, esto conlleva a una brecha de seguridad importante sobre la red de la empresa por que pueden comprometer el uso de todos los equipos conectados sobre él y así mismo los servidores de la compañía, las instalaciones de la escuela presentan fallas en el diseño así como desorganización en los puestos de trabajos evento que facilita que cualquier persona diferente a los funcionarios puedan ver esta información.

La escuela no presenta controles sobre el uso de la internet ni en los servicios de la red corporativa, tampoco cuenta con restricciones de acceso a páginas no productivas, se evidenció que los controles que se realizan no son óptimos sobre la red, ya que implementan métodos sencillos de bloqueos de páginas, utilizando complementos sobre los navegadores, se procede a proponer en forma de diagrama un diseño que ayude a solucionar la falta de seguridad y que ayude a filtrar el tráfico que se genera entre la red y los usuarios como la implementación de un firewall.

Es importante que para salvaguardar el activo más importante que es la información, todos los entes de la Escuela deben trabajar en una sola dirección teniendo el apoyo y respaldo de los entes administrativos, esto con el fin de brindar seguridad en todas las instalaciones ayudándolos a adaptar día a día los nuevos retos que propone el mundo tecnológico.

BIBLIOGRAFIA

BERENGUER SERRATO, David y GARCÍA VALDÉS, Ángela. Estudios de la metodología de ingeniería social [en línea]. España: 2018. [Citado 31-septiembre-2018]. Disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf

BORTNIK, Sebastián. PRUEBAS DE PENETRACIÓN PARA PRINCIPIANTES: 5 HERRAMIENTAS PARA EMPEZAR. Nessus [En Línea]. 2018. [Citado 05-Noviembre-2018] Disponible en https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

COHEN KAREN, Daniel. Importancia de la información para las empresas [En Línea]. Argentina: 2018. [Citado 15-septiembre-2018]. Disponible en https://www.grandespymes.com.ar/2014/10/03/importancia-de-la-informacion-para-las-empresas/

CONFIRMA SISTEMAS. El shoulder surfing, un espionaje muy efectivo [en línea]. 2013. [Citado 03-octubre-2018]. Disponible en https://www.confirmasistemas.es/es/contenidos/canal-basics/el-shoulder-surfing-un-espionaje-muy-efectivo

CORPORACIÓN COLOMBIA DIGITAL. La ingeniería social: el usuario continúa siendo el eslabón más débil [en línea]. 2015., 1 p. [Citado 13-septiembre-2018]. Disponible en https://colombiadigital.net/actualidad/articulos-informativos/item/8556-la-ingenieria-social-el-usuario-continua-siendo-el-eslabon-mas-debil.html

DIGITAL SECURITY. La ingeniería social sigue estando detrás de demasiados ataques [en línea]. 2018. [Citado 31-septiembre-2018]. Disponible en https://www.itdigitalsecurity.es/actualidad/2018/04/la-ingenieria-social-sigue-estando-detras-de-demasiados-ataques

DURIGON, Néstor. Grandes maestros de la estafa. Argentina: Penguin Random House grupo editorial argentina

EL CONGRESO DE COLOMBIA. Artículo 1. (14, octubre, 2003). Concepto de ingeniería. El congreso. Bogotá D.C., 1 p.

EL TIEMPO. Tecnologías evolución y futuro [en línea]. Bogotá: 2018. [Citado 15-septiembre-2018]. Disponible en https://m.eltiempo.com/archivo/documento/MAM-219859

ENTER: CO. La ingeniería social: el ataque informático más peligroso [en línea]. 2018. [Citado 25-septiembre-2018]. Disponible en http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/

ESPITIA, Angélica. Ingeniería social amenaza latente para la seguridad informática [en línea]. Bogotá: 2018, 4 p. [Citado 31-septiembre-2018]. Disponible en http://polux.unipiloto.edu.co:8080/00001891.pdf

FUNDACIÓN UNIVERSITARIA CATÓLICA DEL NORTE. La importancia de los Backups [En Línea]. 2012. [Citado 18-noviembre-2018]. Disponible en: https://www.ucn.edu.co/cpe/r8/sala-prensa/Paginas/La-importancia-de-los-Backups.aspx

GARCÍA VEGA, María. Diversificación tecnológica e innovación [en línea]. España: revista sice. 2018. [Citado 13-septiembre-2018]. 3 p. Disponible en http://www.revistasice.com/CachePDF/ICE_814_49-53__934DE377C1B8A1E00EC612EFF9EEAB24.pdf

GESTION. Siete características para identificar a un ciberdelincuente [en línea]. 2016. [Citado 09-octubre-2018]. Disponible en https://gestion.pe/tecnologia/siete-caracteristicas-identificar-ciberdelincuente-122640

GF0S.COM. Tailgating: acceso a zonas restringidas [en línea]. 2016. [Citado 03-octubre-2018]. Disponible en https://gf0s.com/2016/08/05/tailgating-acceso-a-zonas-restringidas/

GRAÑA, Lara. Alerta frente a las ciberestafas [En Línea]. 2016. [Citado 08-Noviembre-2018] Disponible en https://www.farodevigo.es/economia/2016/08/18/alerta-frente-ciberestafas/1517381.html

HADNAGY, Christopher. Ingeniería Social. El Arte del Hacking Personal. Anaya multimedia.2010

HANSEN, Denis. SAVE Social Vulnerability & Assessment Framework [en Línea]. 2017., 42-49 p. [Citado 15-septiembre-2018]. Disponible en http://www.fak.dk/publikationer/Documents/Project%20SAVE.pdf

INCIBE. La ingeniería social en la empresa: aprovechando la naturaleza humana [en línea]. España: 2014. [Citado 28-septiembre-2018]. Disponible en https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-en-empresas

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Términos y definiciones [en línea]. Bogotá: 2006., 10 p. [Citado 25-septiembre-2018]. Disponible en http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Instituto nacional de ciberseguridad en España. Conoce a fondo qué es el phishing [en línea]. España: 2018. [Citado 13-septiembre-2018]. Disponible en https://www.osi.es/es/banca-electronica

JARAMILLO HINOJOSA, Lucia. Estudio del grado de incidencia de la ingeniería social en la primera fase de los ataques informáticos que se realizan actualmente en las empresas privadas del ecuador. Ecuador.

LEGALITAS. Suplantación de identidad [en línea]. España: 2016. [Citado 03-octubre-2018]. Disponible en https://www.legalitas.com/actualidad/suplantacion-de-identidad

MÉNDEZ, Belisario y NORILEY, Aymara. Análisis de Métodos de Ataques de Phishing. Trabajo de grado en seguridad informática. Argentina: universidad de buenos aires. Facultad de ciencias económicas. 2014. 61 p.

MIFSUD, Elvira. Seguridad de la información / Seguridad informática [en Línea]. España: 2012., 2 p. [Citado 15-septiembre-2018] Disponible en http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

MINTIC. Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información [en línea]. Bogotá: 2016., 15-30 p. [Citado 31-septiembre-2018]. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

MOINELO, Lino. Ingeniería social inversa [en línea]. 2010. [Citado 03-octubre-2018]. Disponible en http://cualeslarealidad.blogspot.com/2010/03/ingenieria-social-inversa.html

NEOATTACK. Concepto de Pop-up [en línea]. Barcelona: 2018. [Citado 03-octubre-2018]. Disponible en https://neoattack.com/neowiki/pop-up/

NORFIPC. Evitar la infección por virus o malware a través del correo electrónico [en línea]. 2018. [Citado 31-septiembre-2018]. Disponible en https://norfipc.com/virus/evitar-infeccion-virus-malware-email-correo-electronico.html

NOTICIAS RCN. Pishing, el método de robo por internet más utilizado en el país [en línea]. Bogotá: RCN. 2018. [Citado 13-septiembre-2018]. Disponible en https://noticias.canalrcn.com/tecnologia-tecnologia/pishing-el-metodo-robo-internet-mas-utilizado-el-pais

PÉREZ PORTO Julián y MERINO, María. Definición de social [en línea]. 2009., 1 p. [Citado 25-septiembre-2018]. Disponible en https://definicion.de/social/

QUEZADA, Alonso. Defensas Contra Ataques De Ingeniería Social [En Línea]. 2017. [Citado 15-Noviembre-2019] Disponible en: http://www.reydes.com/d/?q=Defensas_contra_Ataques_de_Ingenieria_Social

RED SEGURIDAD. ¿Pretexting? los ciberdelincuentes utilizan el teléfono para robar información confidencial [en línea]. 2013. [Citado 03-octubre-2018]. Disponible en http://www.redseguridad.com/actualidad/info-tic/pretexting-los-ciberdelincuentes-utilizan-el-telefono-para-robar-informacion-confidencial

REVISTABYTE. La mitad de ataques de phishing es financiero [en línea]. 2018. [Citado 28-septiembre-2018]. Disponible en https://www.revistabyte.es/actualidad-byte/ataques-phishing-financiero/

ROSE, Karen. LA INTERNET DE LAS COSAS— UNA BREVE RESEÑA. Cuestiones relacionadas con las economías emergentes y el desarrollo [En línea]. 2015. [Citado 28-octubre-2018]. Disponible en https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf

SANDOVAL CASTELLANOS, Edgar. Ingeniería social: corrompiendo la mente humana [en línea]. México: Revista Seguridad. 2010. [Citado 28-septiembre-2018]. Disponible en https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

SANTOS CALDERÓN, Guillermo. Ojo a la ingeniería social [en línea]. Bogotá: El tiempo. 2018., 1 p. [Citado 13-septiembre-2018]. Disponible en https://www.eltiempo.com/opinion/columnistas/guillermo-santos-calderon/ojo-a-la-ingenieria-social-que-afecta-a-las-personas-217088

SANTOS COSTAS, Jesús. Seguridad informática. Editorial y Publicaciones, 2010.

SCOTT SPENCER, James. Ingeniería Social: eludiendo el “firewall humano” [en línea]. México: 2011. [Citado 03-octubre-2018]. Disponible en http://www.magazcitum.com.mx/?p=1173#.W_3bvGhKjIW

SEGURIDAD INFORMATICA ELLA. Ingeniería social inversa [en línea]. 2017. [Citado 03-octubre-2018]. Disponible en http://seguridadinformaticaeya.blogspot.com/2017/03/ingenieria-social-inversa.html

SEGURIDADPC.NET. Concepto de spam [en línea]. 2016. [Citado 31-septiembre-2018]. Disponible en http://www.seguridadpc.net/spam.htm

STANLLING, William. Comunicaciones y Redes de Computadores. 7 ed. México: Prentice Hall 2004

STOLK, Alejandra. Triángulo de debilidades del sistema [en línea]. Bogotá: Es la red. 2013., 40 p. [Citado 15-septiembre-2018]. Disponible en http://www.human.ula.ve/ceaa/temporal/fundamentos_de_seguridad.pdf

TECTECO. Qué es la ingeniería social y cómo afecta a la ciberseguridad [en línea]. España: 2018. [Citado 28-septiembre-2018]. Disponible en https://www.tecteco.com/que-es-la-ingenieria-social-y-como-afecta-a-la-ciberseguridad/

TORRES, Ariel. Hackearán tu mente: Los trucos de ingeniería social que los piratas informáticos usan para cometer fraude, secuestrar archivos y robar tu identidad. Argentina: Grupo Planeta

VOUTSSAS, Juan. Preservación documental digital y seguridad informática [en línea]. México: 2010. [Citado 15-septiembre-2018]. Disponible en http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

WELIVESECURITY. 5 cosas que debes saber sobre la Ingeniería Social [en línea]. 2016. [Citado 28-septiembre-2018]. Disponible en https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/

ANEXO A

V0.1

Nieva, 08 de abril de 2019

Señor:
Juan Carlos Ulloa Quiroga
Coordinador Administrativo y financiero

Asunto: Autorización para la ejecución del proyecto titulado: Identificación De Técnicas De Ingeniería Social Ejecutadas En La Entidad Educativa Esap Huila.

Cordial saludo estimado Coordinador,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a la Escuela Superior de Administración Pública, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: Identificación De Técnicas De Ingeniería Social Ejecutadas En La Entidad Educativa Esap Huila el cual se encuentra avalado por parte la Institución de educación superior "UNAD".

El proyecto en su objetivo general describe lo siguiente: "Analizar la infraestructura tecnológica y los ataques de ingeniería social más frecuentes en la entidad ESAP Huila"; al mismo tiempo será apoyado por los objetivos específicos: "Identificar los ataques informáticos realizado por ingeniería social en la entidad educativa ESAP HUILA, Describir las consecuencias de los ataques informáticos de la ingeniería

social en la entidad ESAP HUILA, Proponer una infraestructura tecnológica que permita detener los ataques informáticos en la entidad ESAP HUILA, Hacer recomendaciones buscando crear buenos hábitos de seguridad en los empleados para lograr disminuir los ataques por ingeniería social en la entidad ESAP HUILA" para obtener como resultado un alto impacto en la seguridad de la empresa Escuela Superior de Administración Pública.

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transaparencia de la ejecución del proyecto:

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por la Escuela Superior de Administración Pública.
- La empresa Escuela Superior de Administración Pública deberá establecer qué tipo de información es privada y cuál es pública para delimintar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de prubas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

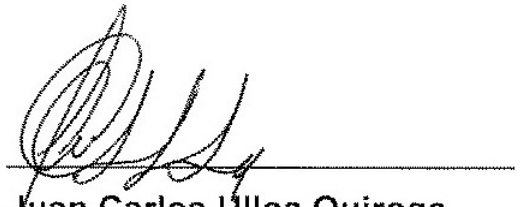
El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El dcumento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en

el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrerar profesional.

Firman en Neiva, a los (08) días del mes de (abril) de 2019

Cordialmente,

Jasson Fabian Oliveros Ortiz
Estudiante UNAD.



Juan Carlos Ulloa Quiroga
Coordinador Administrativo y financiero

ANEXO B

ENCUESTA

CUESTIONARIO SOBRE LA PERCEPCION DE LA SEGURIDAD INFORMATICA EN LA ESCUELA SUPERIOR DE ADMINISTRACIÓN PÚBLICA ESAP

Se busca conocer y determinar el grado de percepción de los usuarios de la institución con temas referentes a la seguridad informática e información en el personal que labora en la escuela superior de administración pública ESAP buscando generar y mejorar las estrategias de la protección de la información y de los sistemas informáticos de la Escuela superior.

Cargo_____

Por favor marque con una "x" su respuesta

ÍTEM	PREGUNTA	OPCIONES DE RESPUESTA			
1	¿Sabe usted que es la ingeniería social y como se aplica?	SI		NO	
2	¿Ha recibido llamadas telefónicas o correos electrónicos que solicitan información personal o confidencial relacionada con la Institución?	SI		NO	
3	¿Confía usted en la solución antivirus que la institución utiliza para los equipos de dotación?	SI	NO	NO SABE	NO USA
4	Teniendo en cuenta que para iniciar sesión en los equipos de la compañía ahí que digitar unas credenciales ¿Cree usted que su contraseña es totalmente segura?	SI	NO	NO SABE	NO USA
5	¿Cree usted que la información que maneja de la institución es importante y confidencial?	SI	NO	NO SABE	
6	¿Considera que el control de acceso físico es idóneo para institución?	SI	NO	NO SABE	
7	¿Su PC está ubicado de tal forma que personas diferentes a usted pueden ver teclado y la información que digita en el monitor donde usted trabaja?	SI	NO	NO SABE	
8	¿Se encuentra su escritorio ordenado la mayor parte del tiempo?	SI		NO	
9	¿Por cuáles de las siguientes amenazas se ha visto afectado dentro de la Institución?	Malware (Virus, gusano y troyanos)			
		Vulnerabilidades o fallas nativas de software			
		Spam (correos no solicitados)			
		Phishing			
		Hackers			
		Spyware			
		Ninguna			
		No sabe			
10	Cual considera usted que es el medio informático más propenso a una amenaza dentro de la institución	Email			
		Redes sociales			
		Chat			
		Navegacion por Internet			
		Descargas			
		No sabe			

ANEXO C

ESCUELA SUPERIOR DE ADMINISTRACIÓN PUBLICA ESAP				
INVENTARIO DE EQUIPOS TECNOLOGICOS E INFORMATICOS				
MAC	**MARCA**	**MODELO**	**AREA**	**SIST.OPERATIVO**
40:61:86:8D:7A:DD	HP	HPPro3000SFF	Biblioteca	Windows 10
F0:4D:A2:EE:A5:F3	HP	HPPro3000SFF	Administrativa Financiera	Windows10
40:61:94:8D:7A:DD	HP	HPProBook4420S	Sistemas	Windows10
00:26:6C:5C:75:50	TOSHIBA	SatelliteL635-SP3001L	Jurídica	Windows10
5C:26:0A:40:CC:63	DELL	LatitudeE6410	Archivo	Windows10
5C:26:0A:40:C7:5F	DELL	LatitudeE6410	Sistemas	Windows10
5C:26:0A:40:C8:67	DELL	LatitudeE6410	Jurídica	Windows10
78:2B:CB:89:B2:14	DELL	Optiplex980	Administrativa	Windows10
78:2B:CB:89:9A:B8	DELL	Optiplex980	Administrativa	Windows10
78:2B:CB:89:B2:14	DELL	Optiplex980	Técnica	Windows10
78:2B:CB:89:9A:0F	DELL	Optiplex980	Administrativa Financiera	Windows10
F0:4D:A2:EE:A6:49	DELL	Vostro320	Asesoría	Windows10
00:1F:16:F9:A4:11	DELL	Vostro320	Asesoría	Windows10
F0:4D:A2:EE:A5:F3	DELL	Vostro320	Archivo	Windows10
F0:4D:A2:EE:A9:46	DELL	Vostro320	Archivo	Windows10

ANEXO D RESUMEN ANALITICO RAE

RESUMEN ANALITICO ESPECIALIZADO	
1. Información General	
Tema	Ingeniería social
Titulo	Identificación de técnicas de ingeniería social ejecutadas en la entidad educativa ESAP Huila
Autor(es)	Reinaldo Enrique Ruiz Duarte Jasson Fabián Oliveros Ortiz
Director	JOHN FREDDY QUINTERO
Fuente Bibliográfica	BERENGUER SERRATO, David y GARCÍA VALDÉS, Ángela. Estudios de la metodología de ingeniería social [en línea]. España: 2018. [Citado 31-septiembre-2018]. Disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf BORTNIK, Sebastián. PRUEBAS DE PENETRACIÓN PARA PRINCIPIANTES: 5 HERRAMIENTAS PARA EMPEZAR. Nessus [En Línea]. 2018. [Citado 05-Noviembre-2018] Disponible en https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar COHEN KAREN, Daniel. Importancia de la información para las empresas [En Línea]. Argentina: 2018. [Citado 15-septiembre-2018]. Disponible en https://www.grandespymes.com.ar/2014/10/03/importancia-de-la-informacion-para-las-empresas/ CONFIRMA SISTEMAS. El shoulder surfing, un espionaje muy efectivo [en línea]. 2013. [Citado 03-octubre-2018]. Disponible en https://www.confirmasistemas.es/es/contenidos/canal-basics/el-shoulder-surfing-un-espionaje-muy-efectivo CORPORACIÓN COLOMBIA DIGITAL. La ingeniería social: el usuario continúa siendo el eslabón más débil [en línea]. 2015., 1 p. [Citado 13-septiembre-2018]. Disponible en https://colombiadigital.net/actualidad/articulos-informativos/item/8556-la-ingenieria-social-el-usuario-continua-siendo-el-eslabon-mas-debil.html DIGITAL SECURITY. La ingeniería social sigue estando detrás de demasiados ataques [en línea]. 2018. [Citado 31-septiembre-2018].

	Disponible en https://www.itdigitalsecurity.es/actualidad/2018/04/la-ingenieria-social-sigue-estando-detras-de-demasiados-ataques DURIGON, Nestor. Grandes maestros de la estafa. Argentina: Penguin Random House grupo editorial argentina EL CONGRESO DECOLOMBIA. Artículo 1. (14, octubre, 2003). Concepto de ingeniería. El congreso. Bogotá D.C., 1 p. EL TIEMPO. Tecnologías evolución y futuro [en línea]. Bogotá: 2018. [Citado 15-septiembre-2018]. Disponible en https://m.eltiempo.com/archivo/documento/MAM-219859 ENTER: CO. La ingeniería social: el ataque informático más peligroso [en línea]. 2018. [Citado 25-septiembre-2018]. Disponible en http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/ ESPITIA, Angélica. Ingeniería social amenaza latente para la seguridad informática [en línea]. Bogotá: 2018, 4 p. [Citado 31-septiembre-2018]. Disponible en http://polux.unipiloto.edu.co:8080/00001891.pdf FUNDACIÓN UNIVERSITARIA CATÓLICA DEL NORTE. La importancia de los Backups [En Línea]. 2012. [Citado 18-noviembre-2018]. Disponible en : https://www.ucn.edu.co/cpe/r8/sala-prensa/Paginas/La-importancia-de-los-Backups.aspx GARCÍA VEGA, María. Diversificación tecnológica e innovación [en línea]. España: revista sice. 2018. [Citado 13-septiembre-2018]. 3 p. Disponible en http://www.revistasice.com/CachePDF/ICE_814_49-53__934DE377C1B8A1E00EC612EFF9EEAB24.pdf GESTION. Siete características para identificar a un ciberdelincuente [en línea]. 2016. [Citado 09-octubre-2018]. Disponible en https://gestion.pe/tecnologia/siete-caracteristicas-identificar-ciberdelincuente-122640 GF0S.COM. Tailgating: acceso a zonas restringidas [en línea]. 2016. [Citado 03-octubre-2018]. Disponible en https://gf0s.com/2016/08/05/tailgating-acceso-a-zonas-restringidas/
Año	2019

Resumen	En el desarrollo de este proyecto se pretende Analizar la infraestructura tecnológica y con ello identificar los ataques informáticos mediante la modalidad de ingeniería social en la entidad educativa ESAP Huila, se revisarán las técnicas de ingeniería social existentes para obtener un análisis de las vulnerabilidades, verificaremos los antecedentes de ataques por ingeniera social en la institución, las cuales se recogerán en un informe para su respectivo análisis. Al terminar la recolección de la información se realizará un análisis con todas las evidencias recolectadas y se genera recomendaciones para crear un hábito seguro entre los trabajadores de las empresas y evitar ser atacadas mediante la modalidad de ingeniería social, así poder aumentar la seguridad en la información. El propósito a lograr mediante la culminación de este proyecto es crear una cultura de seguridad implementando hábitos contra la ingeniería social.
Palabras Claves	Phishing, websites, Ingeniería Social, malware, delincuentes, delitos
Contenidos	Monografía de investigación sobre las diferentes técnicas de ingeniería social usadas por los delincuentes informáticos en Colombia con el fin de detectar las técnicas de este tipo que se están aplicando en la entidad educativa escuela superior de administración pública ESAP sede Huila

2. Descripción del problemas de investigación
Como lo manifiesta María Luz García en su artículo, la diversificación de los sistemas de información en el mundo moderno, y la aparición de importantes medios de comunicación como lo son el internet como medio de comunicación y comercial han obligado a que la seguridad en los sistemas sea cada vez una necesidad obligatoria y a su vez darle importancia a la seguridad que se emplea en los usuarios que son los que dan el manejo al sistema de información de la entidad. Actualmente la ingeniera social según como lo manifiesta la página Colombia digital los usuarios se consideran el enlace más débil dentro del círculo de custodia de activos informáticos, de nada vale tener en nuestros sistemas sofisticados esquema de seguridad, e invertir en firewall y software de seguridad si un funcionario de la entidad no tiene la información y la capacitación necesaria para darle seguridad a su equipo y al acceso de este. En Colombia los ataques más usados utilizando la técnica de ingeniera social se conoce como el phishing (fraude informático que tiene como fin obtener usuarios y contraseñas, mediante suplantación de identidad por medio de correo electrónico SPAM) ese ataque

aumento en un 22.6% entre el 2015 y el 2016 y para el 2017 se estimaba un aumento entre 30 y 40% cada año

Por eso en la entidad ESAP se hace importante identificar los focos de vulnerabilidades ocasionados por problemas de ingeniería social y capacitar al personal para que tenga mayor manejo sobre temas seguridad y con el tener conocimiento de los posibles ataques con ataques de ingeniera social y los riesgos de estos ataques sobre la disponibilidad, confidencialidad e integridad de la información institucional.

El fin es determinar los ataques informáticos que afectan a la Escuela de Administración Pública territorial Huila mediante la modalidad de la ingeniería social, para crear estrategias que prevean estos tipos de ataques y crear un hábito de seguridad informática en la entidad educativa ESAP Huila.

¿Cómo analizando la infraestructura tecnológica traería beneficios para identificar los ataques informáticos mediante la modalidad de ingeniería social en la entidad educativa ESAP Huila?

3. Objetivos

OBJETIVO GENERAL

Analizar la infraestructura tecnológica y los ataques de ingeniería social más frecuentes en la entidad ESAP Huila.

OBJETIVOS ESPECIFICOS

Identificar los ataques informáticos realizado por ingeniería social en la entidad educativa ESAP HUILA.
Describir las consecuencias de un ataque informático por medio de ingeniería social en la entidad ESAP HUILA.
Proponer una infraestructura tecnológica que permita detener los ataques informáticos en la entidad ESAP HUILA.
Hacer recomendaciones buscando crear hábitos de seguridad en los empleados para lograr reducir los ataques por ingeniería social en la entidad ESAP HUILA.

4. Metodología

La monografía se desarrolló en el transcurso de 6 meses entre el segundo semestre del año 2018 y el primer semestre del 2019, esta monografía está dirigida a la identificación

de las técnicas de ingeniería social más utilizadas por los delincuentes informáticos, así como en el planteo de técnicas para ayudar a contrarrestarlas y proponer una infraestructura tecnológica más segura en ESAP con el fin de minimizar los ataques utilizados por ingeniería social.

Su diseño metodológico se basó en 4 fases, la primera fue de autorización y acuerdos de confidencialidad entre la entidad y los estudiantes que realizan la monografía, la segunda fase en una encuesta dirigida a todo los actores con incidencia sobre los equipos informáticos, la 3 fase se basó en la recolección de datos y de información y por último se planearon las actividades para disminuir los ataques por ingeniería social

5. Referentes teóricos

la ingeniera social como técnica de ataque no es indiferente a cualquier otra forma de ataque informático y como tal responde siempre a una metodología básica de funcionamiento donde se refieren siempre la guía a seguir por los atacantes para poder acometer con el objetivo del ataque, para poder describir los pasos a seguir nos basaremos en la propuesta de estudios de la metodología de ingeniería social que se utilizan para describirla básicamente, en ella se describe el período de ataque de una intrusión por ingeniería social en 4 pasos: Selección y reconocimiento, Análisis y contacto, Generación de vector de ataque y explotación y ejecución de vector de intrusión.

Selección y reconocimiento. En esta parte se utiliza una técnica denominada Footprinting la cual tiene como propósito reunir información de la víctima – objetivo utilizando como medio un sitio web clonados para sustraer información, en este paso es muy importante conocer el escenario que se pretende atacar para esta fase es muy importante crear un perfil de la víctima identificar sus hábitos vida, su nivel de intelectualidad, su nivel de confianza antes la gente, su nivel de conocimiento informático y demás.

Análisis y contacto. Con los datos recolectados en el ítem anterior, se realiza un examen minucioso, y se busca hacer contacto con la víctima con el fin de crear un vínculo afectivo con ella y crear una relación de confianza, con el fin de sea relevado la información a la que se quiere acceder.

Desarrollo de la estrategia de ataque y explotación. Creado el lazo de amistad después de efectuarse la fase de selección y reconocimiento, y análisis y contacto, el usuario esta susceptible a una manipulación. Ya se puede generar el ataque de suplantación de identidad y robo de información dando paso a la última fase ejecución de vector e intrusión.

Ejecución de la estrategia e intromisión. Luego de cumplidas las fases de selección, reconocimiento, análisis, contacto, generación de vector de ataques y explotación; La

información es obtenida y los datos del objetivo están vulnerados, logrando dar acceso a la cuenta, sistema, red etc., que planeo atacar. Es importante reconocer e identificar cada etapa que conforman la ingeniera social, ya que esto brindará la ventaja de identificar en que paso considera el atacante que se encuentra con la finalidad de aprender del cómo son sus tácticas sin subestimar su inteligencia y mentalidad, es también importante aprender y aprovechar ese conocimiento para mejorar nuestras habilidades de entendimiento hacia los atacantes.

Para conocer un poco más sobre los temas referentes las ingenierías sociales existen dos tipos de ataques, los que son basados en la tecnología y los que son basados en engaños enfocados al usuario. Los ataques basados en tecnología y en el engaño tienen diferentes niveles de aplicabilidad, siempre está ligado a la víctima que se está atacando.

6. Referentes conceptuales

BASADOS EN LA TECNOLOGÍA

Según lo manifiesta su nombre es la utilización de cualquier medio tecnológico e informático, con el objetivo de realizar el engaño. Sea por aplicación o un sistema alterado por la persona atacante o hacker,

Phishing: Método utilizado por personas para enviar correos o sitios web falsos con el fin de sacar información y realizar estafas. Estos correos suelen hacer creer a las víctimas que vienen de fuentes fiables como entidades bancarias y el único fin que buscan es conseguir información confidencial del usuario para posteriormente realizar algún tipo de fraude.

Email con Código Malicioso. El correo electrónico de forma adjunta puede cargar archivos que tienen código malicioso como malware dentro de estos pueden entrar los que son virus, gusanos entre otros, hay que tener un cuidado especial con este tipo de email, ya que su principal objetivo es infectar el equipo con un malware que permitirá al atacante tener acceso a la información.

“El Propósito que busca es el mismo, lograr insertar de una forma eficaz en el equipo de la víctima software con código malicioso o los llamados spyware, que se define como (spy = espía) (ware = software) se propondrán después de su instalación a capturar las pulsaciones del teclado, al momento de introducir usuarios y password cuando se realiza cualquier tipo de transacción financiera, o de compra o pago por Internet”. Se puede observar en la figura 5 el email con condigo malicioso de forma simbólica.

Spam. Este tipo de correo son considerados los correos basura o también son llamados corres no deseados que normalmente son enviados por remitentes desconocidos y que pueden tornarse molestos, este tipo de correos se generan cuando nos suscribimos a páginas web para solicitar información y ellos actúan sobre nuestras cuentas de correo enviando promociones o novedades sobre sus productos, estos emails spam se pueden

filtrar con código malicioso.
“en definitiva, las direcciones son hurtadas, adquiridas, recogidas en la web o adquiridas de cadenas de mail. Por lo general hay spammers que reenvían un mensaje, también hay numerosos que atacan durante varias semanas con la misma información en el mensaje casi o nadie lee. Muchas de las veces contestar un correo de estos es afirmarle al cibercriminal que nuestro correo está activo y que es válido. Por lo tanto, es recomendable en lo posible hacer caso omiso a este tipo de mensajes y solamente eliminarlos del buzón de mensaje”.

Ventanas emergentes. “O ventana pop-up es el contenido que se genera en las ventanas de navegadores o pestañas de Windows donde se nos muestra información de la cual nosotros no hemos solicitado información, este tipo de información siempre aparece de forma repentina en un navegador web o en la pantalla de tu ordenador. Lo que busca en mostrarte una información complementaria, que consiga enviarnos información de interés o que por el contrario busque reflejar publicidad sobre una marca o negocio” estos pueden ser portadores de infecciones con código malicioso “malware” como virus y troyanos o solamente perturbadores al abrir constantemente ventanas del navegador y mostrar publicidad; Cabe anotar que las mayorías de los navegadores de forma nativa incluyen bloqueadores de pop-up.

Basados en el engaño humano. Es una técnica de la ingeniería social que busca aprovechar las características que como personas nos definen como son el fisgoneo, el temor, la codicia, la concupiscencia la ternura, etc. este es usado con el único objetivo de obtener datos sensibles y confidenciales de la víctima atacada por este método y así vulnerar los sistemas. Estas técnicas pueden pasar desapercibidas para personas sin la capacitación o el entrenamiento adecuado y emplea así “vulnerabilidades en la conducta humana y comúnmente se basan en la sustitución de personas con cierto nivel de autoridad en las empresas”.

Suplantación de identidad. Se entiende como “aquel ejercicio por la que un individuo se hace pasar por otra para realizar acciones de carácter ilegal, como pueden ser solicitar aprobaciones de crédito o préstamo hipotecario, contratar servicios telefónicos o realizar ataques contra otros individuos.” Un ejemplo de esto cuando por medio de una llamada telefónica y con conocimiento previo de la empresa hacerse pasar por un usuario legítimo y solicitar cambios de clave de los correos o equipos de cómputos tal como se verá en la siguiente imagen.

Dumpster Diving. Esta técnica denominada también Búsqueda en la basura es una técnica muy usada, aunque por su nombre suene algo extraño, se trata de encontrar en los restos de las personas información valiosa para su uso y divulgación, este tipo de basura se puede conseguir datos financieros, información de recibos públicos, números telefónicos etc. Para evitar esta técnica es recomendable que tanto como las personas del común

como en las organizaciones es triturar todo el papel que se genera y seguir unos protocolos de seguridad con todo el documento que vaya a ser desechado.

Shoulder Surfing. Técnica basada en espiar por encima del hombro, es un uso muy común y extensamente difundido por las personas que se encargan de hacer ataque por ingeniería social, para su implementación solo es necesario estar ubicado en donde se concurre mucha gente sea bancos, cajeros o sitios públicos como plazas o bibliotecas, y capturar visualmente lo que la víctima digita o escribe. En la actualidad se utilizan programas en dispositivos móviles o cámaras para espiar y tomar fotografías que almacenen la información necesitada, un ejemplo lo podemos ver en la siguiente imagen.

Reverse Social Engineering. “La ingeniería social inversa, se trata de manifestar cómo está hecho un sistema percibiendo cómo es el proceso funcional y las características que este posee. El objetivo es adquirir la mayor cantidad de datos técnicos de un producto del cual no se tiene ningún tipo de información referente tanto a temas de diseño como de sus modelos o esquema interno de este”.
También es usada por los atacantes para realizar problemas en las redes de las empresas teniendo un conocimiento previo sobre la misma, luego ofrece sus servicios para solucionar el problema. Luego el atacante de resolver el problema crea confianza y hace que las victimas siempre estén dependiendo del atacante para dar solución a los problemas de seguridad que se encuentren en la organización.
Esta técnica implica la utilización de tiempo y mucho esfuerzo por parte del ingeniero social o atacante, ya que debe socializar fácilmente, tener buen aspecto y de carácter inofensivo, y sobre todo tener un perfil bajo, así como ser siempre amable y sonreír para tener el agrado de la gente y del personal de las empresas.

Pretexting. Es un método donde el atacante se hace pasar por otra persona sea pública o enrolada en el negocio a vulnerar para poder darle confianza a la víctima y lograr el objetivo de sacar información. “Consiste en la forma de capturar datos y documentos contactando a una empresa y simular ser una determinada persona, con el fin de ser utilizada con actos delictivos”.

Tailgating. Esta técnica que se fundamenta en requerir auxilio directamente de una persona con acceso en la compañía a áreas sensibles para tener acceso a ellas utilizando RFID (identificación por radiofrecuencia), biométrica o algún otro método de identificación. También se utiliza para implementar esta técnica cuando se hacen pasar por personal de la empresa de mantenimiento y entrar áreas restringidas, esta técnica se usa cuando las empresas tercerean ciertos servicios como puede ser de mantenimiento o en el caso cuando las empresas son demasiado grandes.

Deceptive relationships. Para esta técnica lo que busca el atacante es crear un lazo personal para obtener datos importantes de la víctima o de un sistema en general. Para

este ataque solo es suficiente entablar una conversación con la victima crear ciertos patrones de afinidad como gustos, por la música, deporte, autos etc., luego de creado el vínculo intentar extraer información que sea importante para el atacante como direcciones de teléfono sitios de ubicación teléfonos y demás y luego utilizar esta información para atacar a la víctima.

7. Resultados

Para dar un bosquejo inicial sobre la temática que se está tocando en este trabajo se propuso realizar una encuesta con preguntas tipos cerradas y única respuesta (Ver anexo C) para ello se aprovechó las reuniones de área que se hacen con todo el personal antes mencionado donde se incluye los administrativos y docentes que laboran en la institución, solicitando cordialmente de la colaboración de los asistentes para que se pudiera dar con el diligenciamiento del cuestionario ya mencionado.

Se logró aplicar la encuesta a 70 asistentes que respondieron la encuesta satisfactoriamente, se incluyó personal de todas las dependencias de la institución, se excluyó a personal que trabaja con la empresa pero que pertenecen a otras sedes de la organización, solamente se incluyó el personal que trabaja tiempo completo sobre esta sede en Huila, aunque hacen parte de la institución, son un sector que no tiene el 100% del tiempo en la instalación.

Los resultados entregados a continuación son en mayor parte producto de un análisis exhaustivo realizando preguntas enfocadas con el desarrollo de los objetivos planteados por esta monografía para recolectar datos, se diligenciaron las 70 respuestas es un formulario diseñado en Excel desde el cual se implementó la herramienta de tablas dinámicas con el fin de utilizar los diferentes gráficos para entender de una manera adecuada los resultados encontrados. La encuesta se realizó a todos los funcionarios que tienen acceso a los equipos e información de la institución.

8. Conclusiones

La ingeniera social es una técnica no ajena a cualquier persona del medio no importa los estratos económicos ni situación social ella lo que busca siempre es la forma de obtener información de personas sin que ellos sean conscientes de la entrega de datos relevantes sobre un negocio o compañía, estas técnicas son no convencionales y muy efectivas a la hora de sacar información, los ataques pueden ser perpetrados por espías, ciberdelincuentes detectives privados, gente del común, etc.

En este trabajo tratamos de recopilar todas las técnicas que actualmente se utilizan para realizar la ingeniería social de una manera resumida explicar el

concepto de cada una de ellas, con el fin de que el lector pueda entender el concepto y relacionarlo con algunos sucesos de su vida diaria, así mismo identificar las técnicas y cuáles son los métodos que se pueden utilizar en la ESAP

Existen áreas dentro de la institución a las cuales se logra acceder de manera que nadie ni nada ejerce control sobre ellos y estos equipos se encuentran ubicados dentro de áreas sensibles como son las administrativas, lo que permite hacerse fácilmente al control de estos equipos con permisos administrativos y poder realizar un ataque a gran escala dentro de la ESAP

La red de la empresa principalmente la cableada tiene presente múltiples puertos de red habilitados que dan al acceso al público, esto con lleva a una brecha de seguridad importante sobre la red de la empresa por que pueden comprometer el uso de todos los equipos conectados sobre él y así mismo los servidores de la compañía.

Los controles de usuario a los equipos no están basados en ambiente de directorio activo, generando dificultades sobre la administración de ellos, así como los permisos que estos tenga sobre la red de la compañía lo que además con lleva a poder compartir información sin el previo consentimiento de los funcionarios del área de tecnología e informática.

La escuela no presenta controles sobre el uso de la internet ni restricción de acceso a páginas no productivas, se evidencio que los controles que se realizan no son óptimos sobre la red, ya que estos implementan métodos sencillos de bloqueos de páginas utilizando complementos sobre los navegadores, pero se necesita una solución que ayude a filtrar el tráfico que se genera entre la red y los usuarios como la implementación de un firewall.

Muy a pesar que se encontraron backups de los servidores de la escuela, esta no se encuentra preparada para contrarrestar las amenazas que fueron encontradas y mucho menos para implementar un plan de contingencia en caso de una falla total de los sistemas implementados

Es importante que para salvaguardar el activo más importante que es la información, todos los entes de la Escuela deben trabajar en una sola dirección teniendo el apoyo y respaldo total de los entes administrativos, esto con el fin de cambiar la perspectiva brindando seguridad en todas las fases, ayudándonos a adaptarnos día a día a los nuevos retos que propone el mundo tecnológico