UNAH
UNIVERSIDAD NACIONAL
AUTÓNOMA DE HONDURAS

IS-811 | Seguridad Informática

Primer Periodo 2022
Tarea 1-2

Elaborado por:

Tiffany Monique Matamoros Gonzalez

No. Cuenta:

20181002925

Docente:

Ing. Rafael E. Diaz del Valle O.

Índice General

1. Introducción III
2. Problema IV
3. Objetivos IV
   3.1. Objetivo General IV
   3.2. Objetivos Específicos IV
4. Marco Teórico V
   4.1. Definición V
   4.2. Métodos de ataque V
   4.3. Herramientas de identificación y defensa IX
5. Diseño de la Investigación XII
   5.1. Estrategia XII
   5.2. Plan de análisis XII
6. Conclusiones XIII
7. Referencias XIV

1. Introducción

En la actualidad y en el campo de la seguridad informática el término de ingeniería social es muy reconocido, pues sin duda alguna son las compañías las que más resguardan y protegen su información, puesto que es considerada como la columna vertebral de sus negocios y se debe conservar su integridad. Las empresas siempre buscan tomar medidas de seguridad que ayuden a gestionar su información, para ello se tiene en cuenta tres pilares de suma importancia para la seguridad, tales como: la confidencialidad, la integridad, y la disponibilidad.

Herramientas como firewall para aplicaciones (WAF), sistemas de detección de intrusos (IDS), sistemas de protección de intrusos (IPS), entre otras, resultan cada vez más costosas y presentan altos grados de complejidad en su administración; también existe en todas las empresas del mundo un recurso inseguro que almacena información sensible, que es “la mente humana,”. Uno de los más importantes activos de información que se deben identificar en las organizaciones son las personas, pues son estos los que albergan gran cantidad de datos, procedimientos, accesos, y controles que pueden actuar como mecanismos de seguridad o de peligro para el acceso a información. En la actualidad se vive la 4ta revolución industrial que da lugar a una mayor cantidad de trabajos automatizados y un desalojo de capital humano en muchos rubros industrializados, esto puede verse como una ventaja en países donde la ingeniería social juega un papel principal en el hallazgo de vulnerabilidades en sistemas informáticos como ser los países latinoamericanos.

2. Problema

Describir el funcionamiento e implementación de la metodología de Ingeniería Social aplicada a un ataque informático.

3. Objetivos

3.1.Objetivo General

- Determinar cuales son los factores clave que hacen que la ingeniería social represente una brecha de seguridad en sistemas informáticos.

3.2.Objetivos Específicos

- Ampliar los conocimientos referentes a la ingeniería social orientado al rubro informático.
- Analizar como las personas son participes a la hora de encontrar vulnerabilidades en sistemas informáticos.
- Definir formas en las que se puede evitar que las personas representen brechas de seguridad en sistemas informáticos.
- Evaluar vulnerabilidades adyacentes a la ingeniería social para determinar posibles soluciones una vez dichas oportunidades hayan sido aprovechadas...

4. Marco Teórico

4.1. Definición

La definición formal de la ingeniería de software en Según el diccionario Merriam Webster:

1. “La gestión de los seres humanos de acuerdo con su lugar y función en la sociedad.”

2. “Es la aplicación práctica de los principios de la sociología a problemas sociales particulares.”

Otra definición es que la ingeniería social es la práctica para obtener información confidencial, en la mayoría de los casos información de gran valor a través de la manipulación de la mente en las personas, para realizar acciones dentro de un sistema informático cómo ejecutar un software, facilitar sus claves de acceso, o acceder a determinados servicios, donde los atacantes por medio del engaño intentan obtener información sensible o privilegios en algún sistema. Se dice que la ingeniería social consiste en aprovecharse de los demás para recopilar información e infiltrarse en un sistema informático. La naturaleza humana es la mayor proeza del ingeniero social donde aprovecha las vulnerabilidades de las personas para conseguir así cumplir objetivos orientados a un sistema informático.

4.2. Métodos de ataque

Es importante entonces decir que la ingeniería social podría presentarse de dos maneras: una es interactuando con máquinas junto con software y la otra basada en el ser humano por lo que el ataque informático se ve reflejado en dos maneras una social y la otra técnica.

Un ingeniero social puede usar una táctica conocida como ingeniería social inversa. Hay tres partes para revertir la ingeniería social: "sabotaje, publicidad y asistiendo". La ingeniería

social inversa implica crear una situación en la que el atacante debe ayudar al individuo objetivo, o se encuentra en una postura de ofrecerle un producto o servicio de manera publicitaria y el último caso es el del sabotaje en si, donde se aprovechan técnicas de manipulación que demuestran las capacidades sociales del atacante.

Los ingenieros sociales prosperan con información fácilmente alcanzable, como números de teléfono, los ataques exitosos de ingeniería social dependen de los empleados de una organización.

Existen webs con información valiosa donde aprender los métodos para engañar a las víctimas, uno de estos portales es https://socialengineer.org, la ingeniería social no es algo que se pueda eliminar por completo pero lo que sí se puede hacer es mitigarla y la mejor forma de evitarla es no dejarse engañar, los ataques de I.S actúan en dos niveles:

1. El físico: Describe los recursos y medios a través de los cuales se llevará a cabo el ataque.

- Ataque por teléfono o vía SMS
- Shoulder surfing: Se realiza a través de la observación directa ◦ Ataque vía internet: Vía correo, página web, software p2p, mensajería instantánea, hoy en día la mayoría de los ataques provienen del método del correo electrónico.
- Dumpster diving o trashing: Consiste en buscar información relevante en la basura,
- como: agendas telefónicas, organigramas, agendas de trabajo, unidades de almacenamiento (CD, USB, etc.)

- Office snooping: Esta técnica aprovecha la ausencia de la persona responsable de la oficina para husmear en su PC o documentos.
- Ataque cara a cara: El atacante requiere tener una gran habilidad social y extensos conocimientos para poder manejar adecuadamente cualquier situación que se le presente.

2. El psicosocial: El método con el que se engañará a la víctima

- Exploit de familiaridad: Táctica en que el atacante aprovecha la confianza que la gente tiene en sus amigos y familiares, haciéndose pasar por cualquiera de ellos.
- Crear una situación hostil: El ser humano siempre procura alejarse de aquellos que parecen estar locos o enojados, o en todo caso, salir de su camino lo antes posible.
- Conseguir empleo en el mismo lugar: Cuando la recompensa lo amerita, estar cerca de la víctima puede ser una buena estrategia para obtener toda la información necesaria.
- Leer el lenguaje corporal: Un ingeniero social experimentado puede hacer uso y responder al lenguaje corporal.
- Explotar la sexualidad: Técnica casi infalible. Las mujeres que juegan con los deseos sexuales de los hombres poseen una gran capacidad de manipulación, ya que el hombre baja sus defensas y su percepción.

Otra forma que tiene un ciberdelincuente para abordar a sus victimas son en las redes sociales, donde en resumen siguen un flujo como el siguiente:

1. Primero recolectan toda la información posible extrayéndola de las redes sociales

2. Consolidan un plan de ataque para transmitir fiabilidad.

3. Recolectan información particular, entienden su comportamiento (temas de interés, amigos, gustos, etc.), y ganan su confianza.

4. El atacante hace su primer acercamiento (con un falso perfil) teniendo ya definida la táctica de engaño que va a utilizar.

5. Cuando la víctima lo considera "su amigo," el delincuente se muestra cercano y siempre intentará sonsacarle aún más información a través de mentiras

. 6. Una vez siendo "amigos," el ciberdelincuente pedirádatos más personales (correo electrónico, dirección, número de teléfono, etc.).

7. En este punto, la identidad podría suplantar de una manera más rápida y eficiente, o se le enviaría a través de correo electrónico un enlace llamativo que al abrirlo ejecutase un troyano que infecta el computador y diera acceso a las cuentas bancarias de la víctima.

8. Después de obtener lo que buscaba el atacante borra todo rastro, abandona perfiles y no vuelve a hablar con la víctima.

Hay cierta información personal que puede considerarse información sensible, como fotos con ubicaciones y/o lugares frecuentes, direcciones de vivienda o trabajo, nombre de la empresa donde trabaja, nombres de familiares, gustos, y hasta números de celular, la cual se encuentra alojada en redes sociales.

Entre las prácticas más comunes de ataque de ciberdelincuentes están:

1. Phishing: Consiste en enviar correos electrónicos que parecen confiables con el objetivo

de robar información personal y confidencial, se dice que esta modalidad de ataque abarca un 77% de los ataques sociales reportados.

2. Vishing: Consiste en obtener información o generar acciones a través un teléfono móvil o fijo y suele realizarse en prácticas como suplantar la identidad de otra persona.

3. Smishing: Son los ciberdelincuentes que realizan phishing a través de mensajes de texto y buscan hacer caer a la víctima bien sea abriendo un enlace falso.

4.3. Herramientas de identificación y defensa

La forma de defenderse contra estos tipos de ataques de I.S es capacitando y formando a las personas en sus casas, universidades, y aquellas que laboran en las diferentes compañías, para prevenir riesgos que se puedan ocasionar sobre los sistemas informáticos la brecha que puede dejar de vulnerabilidades el capital humano. Mecanismos validos para la prevención de riesgos:

- Nunca divulgar información sensible con desconocidos o en lugares públicos.
- Si se sospecha que alguien intenta realizar un engaño, hay que exigir se identifique y tratar de revertir la situación intentando obtener la mayor cantidad de información del sospechoso y sin alertarlo.
- Implementar un conjunto de políticas de seguridad en la organización que minimice las acciones de riesgo, y comunicarlas a todos los funcionarios de la compañía.
- Efectuar controles de seguridad física para reducir el peligro inherente a las personas.
- Realizar rutinariamente auditorías y pen test usando I.S para detectar huecos de seguridad de esta naturaleza.
- Llevar a cabo programas de concientización sobre la seguridad de la información.

- Políticas de contraseña
- Evaluaciones de vulnerabilidad
- Clasificación de datos
- Política de uso aceptable
- Verificaciones de antecedentes
- Proceso de terminación
- Respuesta al incidente
- Seguridad física
- Capacitación en conciencia de seguridad.

Para un ingeniero social, obtener acceso a un sistema puede significar la diferencia entre un ataque exitoso o fallido. Una buena política de contraseñas debe incluir información acerca de:

- No compartir contraseñas cuando se le pregunta
- No escribir contraseñas
- No usar contraseñas predeterminadas
- Métodos para identificar usuarios para restablecer contraseñas
- Métodos para la entrega de contraseñas
- Creación de contraseña, es decir, longitud mínima, alfanumérica
- Asegurar la estación de trabajo con un protector de pantalla protegido por contraseña antes de salir de un espacio de trabajo
- Cambio periódico de contraseña
- Período de gracia para contraseñas que caducan

- Bloqueo por falla de inicio de sesión, es decir, la cuenta se bloquea después de 3 intentos fallidos.
- Estándares de contraseñas administrativas y del sistema Existes distintas formas de mitigar las consecuencias de un ciber delicuente que se valga mayormente de la ingeniería social para realizar sus ataques, por ejemplo existen herramientas como messageheader de Google, messageheader analyzer de Microsoft en donde se puede revisar que los dominios de confianza no sean suplantaciones de otros, esto a través de campos como:
- **Received**: Muestra una lista de todos los servidores y ordenadores por las que el correo ha viajado para llegar al destinatario.
- **X-Spam-Status o X-Spam-Level:** Esto muestra la puntuación de Spam generada por tu servicio o cliente de correo.
- **X-Mailer:** En algunos clientes de correo o plataformas se puede visualizar desde que cliente de correo se ha enviado el mail.

5. Diseño de la Investigación

5.1. Estrategía

- **Investigación-Acción**: Dentro del marco de los estudios en enseñanza de lenguas, podemos encontrar investigaciones que se enfocan en detectar un problema para después proponer un tratamiento o un mejor acercamiento para solucionar dicho problema.

5.2. Plan de análisis

- Conocer la definición y distintas interpretaciones de la ingeniería social
- Definir las formas en las que los ciberdelincuentes hacen uso del capital humano para aprovechar vulnerabilidades sistemas de información
- Determinar estrategias a seguir para mitigar las vulnerabilidades que se puedan aprovechar por un ciberdelincuente.

6. Conclusiones

- La ingeniería social pasa por alto las tecnologías implementadas para proteger y detectar actividades maliciosas. Es una amenaza que siempre existirá y que no puede ser contenida por un software antivirus, parches completos, firewalls y sistemas de detección de intrusos. Solo se necesita un empleado desprevenido para que un ataque de ingeniería social tenga éxito y, como resultado, convierte a los empleados en el eslabón débil de una política de seguridad.
- El inconveniente de la ingeniería social es un mal que no tiene una cura, sino solamente un tratamiento, con la capacitación adecuada y las políticas implementadas, el riesgo de la ingeniería social se puede mitigar de manera efectiva.
- La concientización masiva es una de las formas en las que se le puede hacer frente a la ingeniería social aplicada a la extracción de información delicada del capital humano ya sea de una empresa o de forma individual

7. Referencias

- Security check. (2017, 1 octubre). Base de Conocimiento, Entender Una Cabecera de Correo. https://help.clouding.io/hc/es/articles/360011403640-Entender-una-cabecera-de-correo
- Ingeniería social, hackeando a personas. Sitio web. [Online]. Disponible: https://csirt.utpl.edu.ec/ingenieria#social-hackeando-personas
- Colom, J. L. (2022, 2 febrero). La IoT (Internet de las cosas) y sus implicaciones éticas, legales y de seguridad. Aspectos profesionales: Protección de Datos, Cloud Computing y Sistemas de Gestión. http://www.aspectosprofesionales.info/2014/01/
- Houston. (2021, 20 agosto). ¿Cómo funciona la Ingeniería Social? Mr. Houston Tech Solutions. https://mrhouston.net/blog/como-funciona-la-ingenieria-social