Ingeniería Social

Diego Corredor, Cristian López, Pedro Mayorga, Luis Pizza, estudiantes, Escuela Colombiana de Ingeniería Julio Garavito

***Resumen*—Para el desarrollo practico de nuestro proyecto de ingeniería social, realizaremos un ataque de phishing, explotando la vulnerabilidad del sistema de correo de la universidad escuela colombiana de ingeniería julio Garavito, el objetivo es demostrar la alta vulnerabilidad que presenta el correo y como pueden obtenerse datos sensibles de los estudiantes con cierta facilidad por parte de los atacantes.**

***Abstract*—In the practical development of our social engineering project, we will carry out a phishing attack, exploiting the vulnerability of the mail system of the Escuela Colombiana de Ingenieria Julio Garavito university, the main goal is to demonstrate the high vulnerability that mail presents and how sensitive data can be obtained of students with some ease.**

I. INTRODUCCIÓN

Últimamente la universidad se ha visto afectada por diversos ataques de phishing mediante el correo institucional. A pesar de que tales ataques han sido en su implementación bastante limitados, una gran parte de la población de estudiantes han sido engañados, cediendo sus datos personales a los atacantes, lo cual presenta un gran riesgo para toda la institución. Por lo anterior mencionado decidimos enfocarnos en la implementación de varios ataques de phishing, los cuales tendrán como objetivo obtener las contraseñas de los correos de los estudiantes, para también verificar si usan estas mismas contraseñas en otras cuentas personales como Facebook, Twitter, Instagram.

Se enunciará la metodología que usaremos, el estudio realizado a la población y las herramientas que se utilizaran para la ejecución de este.

II. OBJETIVOS

- Demostrar la vulnerabilidad de la universidad frente a ataques de phishing.
- Implementar varios ataques certeros de phishing utilizando diversas técnicas de ingeniería social.
- Analizar los datos recolectados en el ataque para proponer estrategias de prevención dentro de la comunidad educativa.
- Definir el ataque con mayor impacto y efectividad dentro de los propuestos.

III. MARCO TEÓRICO

Phishing (Suplantación de Identidad): Es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima. El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

Red Team: Es un equipo humano, que realiza ataques (siempre controlados) a un objetivo, que ha sido definido anteriormente por parte del cliente y bajo un contrato de confidencialidad y de alcance del mismo. El red team debe representar una amenaza real, constante en el tiempo, como si de una monitorización se tratase.

Perfilamiento de población: Es un proceso mediante el cual se adquiere un conocimiento sobre los usuarios objetivo del ataque, de forma que el ataque y sus respectivas pruebas son de una personalización mucho mayor y se adaptada al comportamiento de los usuarios de la aplicación o servicio, sus gustos, intereses, etc.

IV. METODOLOGÍA

1. Estudio de población objetivo.
2. Perfilamiento para la dirección del ataque.
3. Duplicación de página web.
4. Envió de notificación.
5. Obtención de información (número de teléfono, correo electrónico personal, contraseña).
6. Análisis de datos obtenidos.

V. DESARROLLO

Estudio de población objetivo:

La población objetivo serán los estudiantes de la escuela colombiana de ingeniería julio Garavito. El estudio y la obtención de información se realizará por medio de unas encuestas en la que los estudiantes nos suministraran datos personales de gran importancia como lo es el correo electrónico

(puede ser el personal o institucional) y otros no tan transcendentes para ellos como: gustos del estudiante, actividades que realicen en sus tiempos libres, temas de agrado, hobbies, entre otros datos los cuales sean y/o consideremos relevantes para la planeación y materialización del ataque. Como ya se mencionó antes se realizarán diversas encuestas, esto con el objetivo de lograr conseguir un número Importante de estudiantes encuestados el cual nos permita tener mayor probabilidad de un ataque exitoso.

Perfilamiento para la dirección del ataque:

Una vez culminado el estudio de la población objetivo, mediante los datos suministrados por los estudiantes realizaremos un agrupamiento de los mismos acordes a sus gustos, hobbies y demás datos que nos permitan tener grupos de estudiantes que cuenten con intereses afines y/o relacionados. Un realizado dicho agrupamiento procederemos a realizar un estudio de los grupos de intereses y se planteara una idea de publicidad, promoción o marketing para cada grupo. Esto nos permitirá proceder a la siguiente fase.

Duplicación de página web:

Una vez realizado el perfilamiento de los estudiantes objetivos y el estudio de los grupos de interés de los estudiantes, Se comenzará con el desarrollo de las páginas web de acuerdo con las promociones o publicidad que se vayan a realizar mediante una estrategia de suplantación, se tomara una empresa referente en la que se realizara una duplicación de esta adaptada a la estrategia seleccionada de obtención de información esto con el fin de generar confianza visual por parte de las victimas al momento de entrar al sitio web, donde podrán conocer y acceder a la supuesta promoción.

Envío de notificación:

En este pase procederemos a ejecutar el ataque, se les notificara a los estudiantes que realizaron la encuesta vía correo o red social, donde se les informara de la que ya está disponible la promoción ofrecida dando les un enlace de redirección a la página web realizada.

Obtención de Información:

Una vez en el sitio web, se les solicitará a los estudiantes que creen una cuenta y la sincronicen con la institucional para verificar que, sí son estudiantes, una vez realizado se les dará un código con el cual podrán redimir la "promoción" ofrecida en cualquier punto físico de la tienda o local. De esta manera se obtendrán no solo datos de la cuenta institucional, sino además datos personales como el correo o el teléfono.

Análisis de datos obtenidos:

Una vez terminado el proceso se revisará cuantos estudiantes cayeron en el phishing propuesto para de esta manera analizar el nivel de seguridad con el que gestionan las cuentas personales que tienen, así como el uso de contraseñas diferentes para cada sitio o si usan la misma para todo, que tan enlazada tienen la información en los datos suministrados y que se puede obtener de información privada de cada uno de ellos.

VI. HERRAMIENTAS

- **Trape:** Herramienta de reconocimiento que te permite rastrear a las personas y hacer ataques de phishing en tiempo real, la información que puedes obtener es muy detallada.
- **BlackEye:** Actualización de la herramienta ShellPhish, es la herramienta de phishing más completa, con 32 plantillas personalizables.
- **SocialFish:** Herramienta de phishing educativa y recopilador de información.
- **Heroku:** Plataforma de cloud computing donde se desplegará el formulario de recolección de datos duplicado.
- **Github:** Servicio de alojamiento de proyectos para usar junto a Heroku.
- **Instagram:** Red social donde comprobaremos las credenciales obtenidas del ataque.
- **Facebook:** Red social donde comprobaremos las credenciales obtenidas del ataque.
- **GetResponse:** Herramienta para el envío masivo de correos electrónicos.
- **MailRelay:** Herramienta para el envío masivo de correos electrónicos.
- **MDirectory:** Herramienta para el envío masivo de correos electrónicos.
- **JAVA:** Lenguaje de programación que se usará para enviar peticiones a redes sociales con las credenciales obtenidas del ataque.

VII. CONCLUSIONES

Con base a la metodología ya definida anteriormente, se espera realizar un ataque exitoso que muestre las vulnerabilidades de un sistema real cómo es el servicio de correo de la escuela, así como el sistema de servicios académicos.

De esta manera, se busca llevar a cabo un ataque robusto y certero a la seguridad de los estudiantes que mediante el uso de ingeniería social obtenga datos sensibles de los mismos que permitan analizar no solo el riesgo de la plataforma actual, sino los posibles impactos de que esta posible situación de ataque se materialice a manos de delincuentes informáticos.

Como equipo de Red Team, se busca que esta prueba de ataque nos brinde la información y datos necesarios para saber cómo actuar ante un posible ataque y así proteger el sistema que controla a todos los usuarios que tiene la escuela.

VIII. BIBLIOGRAFÍA

antevenio. (s.f.). Obtenido de antevenio: https://www.antevenio.com/blog/2017/04/los-mejores-software-para-envio-masivo-de-email/

avast. (s.f.). Obtenido de avast: https://www.avast.com/es-es/c-phishing

Ayuda Ley Protección Datos. (s.f.). Obtenido de Ayuda Ley Protección Datos: https://ayudaleyprotecciondatos.es/2018/09/10/suplantacion-identidad/

b-secure. (s.f.). Obtenido de b-secure: https://www.b-secure.co/recursos/infografias/tecnicas-y-ataques-de-ingenieria-social

Deusto Facultad de Ingeniería. (s.f.). Obtenido de Deusto Facultad de Ingeniería: https://blogs.deusto.es/master-informatica/el-perfilado-de-usuarios-y-la-privacidad/

ICEMD. (s.f.). Obtenido de ICEMD: https://www.icemd.com/digital-knowledge/articulos/red-team-experiencia-en-ataque/

SEGU.INFO. (s.f.). Obtenido de SEGU.INFO: https://www.segu-info.com.ar/malware/phishing.htm

Web Site Tool Tester. (s.f.). Obtenido de Web Site Tool Tester: https://www.websitetooltester.com/es/blog/programas-para-enviar-correos-masivos/#MailRelay_Envia_hasta_75000_emails_gratis

Wikipedia. (s.f.). Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Phishing

Wikipedia. (s.f.). Obtenido de Wikipedia: https://es.wikipedia.org/wiki/GitHub

Wikipedia. (s.f.). Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Heroku