# Social Security Risk

Sandra Milena Jerez Valero
Mauricio Díaz Torres
Maestría en Seguridad de la Información
Universidad de los Andes, Colombia
Junio 2023

## Resumen

"*La ingeniería social se refiere al uso de técnicas y acciones premeditadas para manipular las acciones de las personas, persuadiéndolas a realizar tareas que normalmente no harían*" [1]. Siguiendo esta premisa, los ciberdelincuentes se aprovechan para enviar correos electrónicos tipo phishing, convencer a sus víctimas y obtener acceso sin dificultad al sistema de información. Por tanto, es clave estar preparados para detectar este tipo de ataques y realizar en las empresas ejercicios controlados de entrenamiento.

Actualmente estos ejercicios de ingeniería social no tienen un alcance suficiente porque las empresas de consultoría contratadas para realizar adelantar estos ejercicios, o el uso de las herramientas existentes que soportan las tareas asociadas, se limitan a enviar un correo prediseñado a un grupo objetivo y entregar un informe que resume quién accedió al enlace o quién proporcionó la contraseña. Este trabajo propone aumentar el alcance de estos ejercicios, es decir, no solamente entregar un informe estadístico, sino más bien, entregar un perfil de riesgo de esa persona que accede al enlace y entrega la contraseña, ya sea usando los privilegios que pudiera tener, el rol que desempeña en la compañía o características dela contraseña y generar recomendaciones que ayuden a las empresas a tomar mejores decisiones a la hora de realizar campañas de sensibilización, robustecer los controles de seguridad existentes y gestionar riesgos que puedan darse.

## 1. Introducción

Viviendo en una sociedad estamos expuestos a la manipulación, a ser influenciados para tomar ciertas decisiones; decisiones que no siempre son por nuestro propio bien o por el bien común. Esta realidad no es necesariamente negativa, ya que desde temprana edad se educa en este contexto: atender órdenes y seguir a líderes o referentes. Los ataques de ingeniería social aprovechan esta dinámica, y eso los hace muy efectivos y les permite mantener su relevancia a lo largo del tiempo. Estadísticas que indican que el 90% de los ciberataques tienen su origen en un fallo humano de seguridad [3], no suenan descabelladas y están relacionadas con la efectividad de los ataques de ingeniería social.

El phishing, es una de las técnicas comúnmente empleadas en la ingeniería social, la cual consiste en enviar un correo electrónico persuasivo que contiene un enlace a un sitio web falso para que la víctima ingreses datos como usuario y contraseña de acceso. Según el informe DBIR [4] de 2022, se ocasionaron aproximadamente 2,249 incidentes de esta naturaleza, de los cuales, en 1,063 se confirmó la exfiltración de datos de la compañía. A pesar del impacto que tiene este tipo de escenarios, la única solución plausible para mitigar este factor de riesgo es concienciar a las personas en las buenas prácticas de seguridad al usar tecnología digital [3].

En la actualidad, compañías especializadas en seguridad, como 2Secure, incluyen en su portafolio de concientización servicios como:

- Piezas enviadas vía correo electrónico a los colaboradores con recomendaciones de seguridad.
- Charlas explicativas sobre ingeniería social.
- Campañas de phishing, donde el cliente proporciona el alcance, temática.
- Otros tipos de ejercicios de ingeniera social como smishing, vishing, QRLjacking, etc.

Otra estrategia que han adoptado las compañías es la adquisición de herramientas, pagas o gratuitas, para realizar simulaciones de phishing, por ejemplo, *Attack Simulator*, una herramienta de Microsoft (tiene un costo de acuerdo con el modelo de licenciamiento que tenga una compañía) o *GoPhish*, herramienta *open source*.

El resultado de cualquiera de estas herramientas es un informe con estadísticas y recomendaciones genéricas de seguridad que pueden o no aplicar a la compañía. Es necesario ir más allá de esta visión general y considerar las consecuencias en caso de compromiso de cuentas de usuario, y enfocarse en situaciones más específicas para identificar los riesgos asociados, mitigarlos de la mejor manera e intentar minimizar la cantidad de incidentes que puedan presentarse.

## 2. Propuesta

Como solución al problema identificado, este trabajo propone el desarrollo de una herramienta de software, orientada a medianas y grandes empresas, que permita llevar a cabo pruebas de escenarios de ataque de ingeniería social y, adicionalmente, permita evaluar el nivel de riesgo de los empleados de una compañía en función de los resultados obtenidos en cada escenario.

### 2.1 Diseño

Los requerimientos funcionales identificados para esta herramienta incluyen: envío de correos, recolección de información, generación de informe, importar plantilla, implementar plantillas por defecto, alimentar módulos, extracción de datos del sistema de información de la compañía, control de acceso al sistema, estructuración y limpieza de los datos, evaluación de riesgo por cuenta de usuario, evaluación de riesgo por la compañía en general, generación de recomendación, extracción de resultados, minimizar falsos positivos en correo electrónico, minimizar falsos positivos en contraseñas, cantidad de usuarios por ejercicio, construir un pretexto de acuerdo con información obtenida, importar el listado de usuarios objetivo del y crear el hosting del sitio web. Los requerimientos no funcionales son: usabilidad de la aplicación, adaptable a las necesidades del cliente, confidencialidad de la información y accesibilidad.

Con base en los requerimientos identificados, se propone una herramienta que consta de los siguientes módulos:

- Módulo de OSINT: obtiene información expuesta en internet sobre los empleados de la compañía, incluyendo perfiles de redes sociales, direcciones de correo electrónico, números de teléfono, entre otros para ser utilizados en el módulo de Phishing y Smishing.
- Módulo de Phishing: simula ataques de phishing mediante el envío de correos electrónicos falsos para obtener información confidencial de los empleados.
- Módulo de Smishing: simula ataques de ingeniería social a través de mensajes de texto para obtener información confidencial de los empleados.
- Módulo de Análisis de Riesgo: para evaluar los resultados del Módulos de Phishing y Smishing y perfilar el riesgo de cada empleado, tomando en cuenta factores como: si cayó en la trampa o ingresó a un portal falso e introdujo sus credenciales, los privilegios, accesos disponibles y el rol de cada empleado dentro de la compañía. La herramienta tendrá la capacidad de extraer datos de los sistemas de información de la compañía para identificar qué empleado tiene más privilegios y, por ende, mayor riesgo para la compañía.

La figura siguiente ilustra la interacción de los módulos.

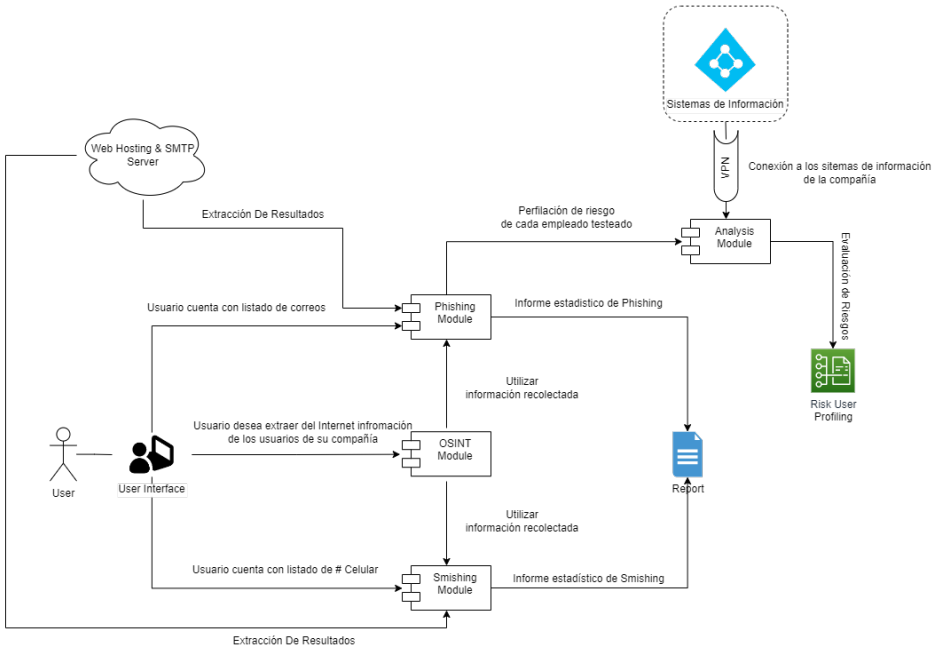



*Figura 1: Diseño general*

El reporte generado incluye los valores calculados para probabilidad e impacto asociados a las acciones de cada usuarios de la compañía. A continuación, se explica cómo se estiman estos valores.

La probabilidad se calcula con base en las situaciones registradas para cada cuenta de usuario evaluada en un ejercicio de ingeniera social. La siguiente tabla presenta los posibles valores y las condiciones de asignación.

| | Bajo (1) | Medio (3) | Alto (6) | Muy Alto (10) |
|---|---|---|---|---|
| **Calificación Cualitativa** | Nunca se ha presentado alguna situación con la cuenta de usuario | Se ha presentado al menos una vez en el año alguna situación con la cuenta del usuario. | Se ha presentado a lo más 2 situaciones en el año con la cuenta del usuario. | Se ha presentado más de situaciones en el año con la cuenta del usuario. |
| **Calificación en términos de oportunidad de que algo suceda** | | Si al menos abrió el correo e hizo clic en el enlace<br><br>Si la cuenta se ha visto comprometidos por violaciones de datos y se obtiene el usuario a través de fuentes OSINT | Si hace más de dos meses que no cambia la contraseña<br><br>Si la cuenta se ha visto comprometidos por violaciones de datos y se obtiene el usuario y/o el hash a través de fuentes OSINT | Si la cuenta proporciona las credenciales de acceso en ejercicios de ingeniera social.<br><br>Si la cuenta se ha visto comprometidos por violaciones de datos y se obtiene la contraseña a través de fuentes OSINT<br><br>Es kerberoastable o ASP-REP Roastable |

El impacto se calcula con base en una matriz que considera principalmente factores financieros y reputacionales, de la siguiente manera:

| | Bajo (1) | Medio (3) | Alto (6) | Muy Alto (10) |
|---|---|---|---|---|
| **Calificación Cualitativa** | Sin esfuerzo ni gasto para recuperarse | Requiere poco esfuerzo o gasto para recuperarse | Requiere esfuerzo o gasto para recuperar y mitigar. | Daño significativo a la compañía. |
| **Calificación en términos financieros** | Impacto financiero hasta el 1% OPEX, dentro de 12 periodo de un mes<br><br>No hay perdida de información. | Impacto financiero desde 1.1% hasta el 5% OPEX, dentro del plazo de 12 meses.<br><br>Pérdida de información no crítica para la compañía. | Impacto financiero desde 5.1% hasta el 15% OPEX, dentro de un período de 12 meses.<br><br>Pérdida parcial de información importante o crítica para la compañía. | Impacto financiero >15% OPEX dentro de un período de 12 meses.<br><br>Pérdida total de información crítica para la compañía. |
| **Ejemplo:** | Cuenta con ningún privilegio relevante y ron de acceso a información pública o no crítica para la compañía. | Cuenta con mínimo privilegio, rol con acceso a información no crítica de la compañía. | Cuenta con:<br>• Privilegio VPN.<br>• Rol con acceso parcial a información importante o crítica de la compañía.<br>• Cuenta con privilegio de RDP | Cuenta con:<br>• Perfil administrador o cuenta de servicio.<br>• Rol con acceso a información crítica de la compañía.<br>• Cuenta con privilegio de RDP. |

Con base en las dos tablas anteriores se hace un cálculo del promedio entre probabilidad e impacto.

## 3. Implementación

En cuanto a la implementación, la herramienta se desarrolla en lenguajes de programación de alto nivel como Python junto con las librerías:

- Ldap3: Librería compatible con Python 2 y Python 3, la cual permite interactuar con el servidor LDAP. Para que pueda funcionar correctamente usa el paquete pyasn1, para comunicarse con el servidor a través de la red. Igualmente, los datos recibidos del servidor

se decodifican con un decodificador ASN1 interno, considerado mucho más rápido que el decodificador pyasn1. El uso de ldap3 es relativamente sencillo: define un objeto de servidor y un objeto de conexión. Luego emite comandos a la conexión y permitir la interacción con LDAP [5]

- Pandas: Librería en cargada de manejo y análisis de estructuras de datos. Esta librería es empleada para la lectura y escritura de los archivos que se van generando en cada uno de los módulos de la aplicación. [6]
- Crackmapexec: Es una utilidad basada en Python para descubrir y explotar las debilidades en la seguridad de Active Directory.[7]
- Password-strength: Encargado de probar e identificar realmente la complejidad de la contraseña con base en política de contraseñas configuradas en este objeto.

**Implementación del módulo OSINT:** Se realizó la integración con tres fuentes OSINT, Deshashed, hunter.io, Intelligence X. Se optó por utilizar APIs pagas en lugar de herramientas de código abierto debido a varios factores:

- Las APIs pagas ofrecen datos más confiables y de mayor calidad que las herramientas de código abierto.
- Brindan acceso a una amplia gama de fuentes de datos, lo que garantiza una cobertura más completa y datos exclusivos.
- Las APIs pagas proporcionan soporte técnico y actualizaciones regulares, lo que garantiza un funcionamiento confiable de la herramienta.
- Ofrecen planes flexibles y permiten escalar el uso de la herramienta según las necesidades del proyecto.
- Tienen acuerdos y términos de uso claros para garantizar el cumplimiento legal y ético en la recolección y uso de datos.

La fuente paga Deshashed, es un API paga que permite realizar búsquedas ilimitadas y obtener información como email, direcciones IP, contraseñas, hash de la contraseña. La conexión se establece de la siguiente manera:

```
# ==============================================================================
#    DEHASHED Collectors
# ==============================================================================

def DEHASHED_SEARCH(domain, page, API_KEY):
    url = 'https://api.dehashed.com/search?query=domain:'+domain+'&size=10000&page='+str(page)

    headers = {
      'Accept': 'application/json',
      'Authorization': 'Basic '+API_KEY
    }

    r = requests.request("GET", url, headers=headers)
    if r.status_code == 200:
        r = r.json()
        return r, r['total']
    else:
        return r.status_code
```

*Figura 2: Código fuente para conexión a API Dehashed*

La fuente paga hunter.io es una herramienta para encontrar direcciones de correo electrónico por dominio y obtener información de contacto. La conexión se establece de la siguiente manera:

```
# ============================================================================
#    Hunter.io Collectors
# ============================================================================

def HUNTER_SEARCH(domain, API_KEY):
    r = requests.get('https://api.hunter.io/v2/domain-search?domain='+domain+'&api_key='+API_KEY)
    if r.status_code == 200:
        return r.json()
    else:
        return r.status_code
```

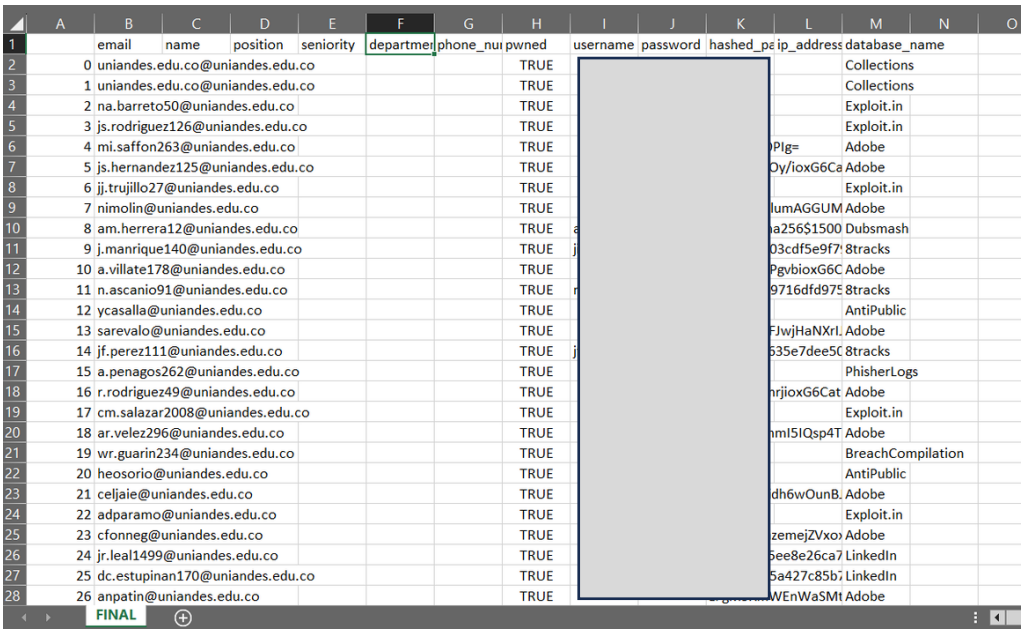
*Figura 3: Código fuente para conexión a API Hunter.io*

La fuente Intelligence X es un API que permite realizar búsquedas exhaustivas en diferentes fuentes, recopilar información como email, direcciones IP, información de contacto y otras, disponibles en internet. La conexión se establece de la siguiente manera:

```
# ============================================================================
#    IntelligenceX Collectors
# ============================================================================

def PHONEBOOK_SEARCH(term, API_KEY, maxresults=100, buckets=[], timeout=5, datefrom="", dateto="", sort=4, media=0, terminate=[], target=0):
    """
    Initialize a phonebook search and return the ID of the task/search for further processing
    """
    h = {'x-key': API_KEY, 'User-Agent':'IX-Python/0.5'}
    p = {
        "term": term,
        "buckets": buckets,
        "lookuplevel": 0,
        "maxresults": maxresults,
        "timeout": timeout,
        "datefrom": datefrom,
        "dateto": dateto,
        "sort": sort,
        "media": media,
        "terminate": terminate,
        "target": target
    }
    r = requests.post('https://2.intelx.io/phonebook/search', headers=h, json=p)
    if r.status_code == 200:
        return r.json()['id']
    else:
        return r.status_code
```

*Figura 4: Código fuente para conexión a API* Intelligence X

Al agrupar la información de estas fuentes, se obtiene un archivo *csv* que contiene la siguiente información, se toma como ejemplo el dominio uniandes.edu.co:



| | email | name | position | seniority | departmer | phone_nu | pwned | username | password | hashed_pa | ip_address | database_name |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | uniandes.edu.co@uniandes.edu.co | | | | | | TRUE | | | | | Collections |
| 1 | uniandes.edu.co@uniandes.edu.co | | | | | | TRUE | | | | | Collections |
| 2 | na.barreto50@uniandes.edu.co | | | | | | TRUE | | | | | Exploit.in |
| 3 | js.rodriguez126@uniandes.edu.co | | | | | | TRUE | | | | | Exploit.in |
| 4 | mi.saffon263@uniandes.edu.co | | | | | | TRUE | | | | )PIg= | Adobe |
| 5 | js.hernandez125@uniandes.edu.co | | | | | | TRUE | | | | Oy/iox G6Ca | Adobe |
| 6 | jj.trujillo27@uniandes.edu.co | | | | | | TRUE | | | | | Exploit.in |
| 7 | nimolin@uniandes.edu.co | | | | | | TRUE | | | | lumAGGUM | Adobe |
| 8 | am.herrera12@uniandes.edu.co | | | | | | TRUE | a | | | a256$1500 | Dubsmash |
| 9 | j.manrique140@uniandes.edu.co | | | | | | TRUE | j | | | 03cdf5e9f7 | 8tracks |
| 10 | a.villate178@uniandes.edu.co | | | | | | TRUE | | | | PgvbioxG6C | Adobe |
| 11 | n.ascanio91@uniandes.edu.co | | | | | | TRUE | r | | | 9716dfd975 | 8tracks |
| 12 | ycasalla@uniandes.edu.co | | | | | | TRUE | | | | | AntiPublic |
| 13 | sarevalo@uniandes.edu.co | | | | | | TRUE | | | | FJwjHaNXrl | Adobe |
| 14 | jf.perez111@uniandes.edu.co | | | | | | TRUE | j | | | 535e7dee5( | 8tracks |
| 15 | a.penagos262@uniandes.edu.co | | | | | | TRUE | | | | | PhisherLogs |
| 16 | r.rodriguez49@uniandes.edu.co | | | | | | TRUE | | | | hrjioxG6Cat | Adobe |
| 17 | cm.salazar2008@uniandes.edu.co | | | | | | TRUE | | | | | Exploit.in |
| 18 | ar.velez296@uniandes.edu.co | | | | | | TRUE | | | | hml5IQsp4T | Adobe |
| 19 | wr.guarin234@uniandes.edu.co | | | | | | TRUE | | | | | BreachCompilation |
| 20 | heosorio@uniandes.edu.co | | | | | | TRUE | | | | | AntiPublic |
| 21 | celjaie@uniandes.edu.co | | | | | | TRUE | | | | dh6wOunB | Adobe |
| 22 | adparamo@uniandes.edu.co | | | | | | TRUE | | | | | Exploit.in |
| 23 | cfonneg@uniandes.edu.co | | | | | | TRUE | | | | zemejZVxo | Adobe |
| 24 | jr.leal1499@uniandes.edu.co | | | | | | TRUE | | | | 5ee8e26ca7 | LinkedIn |
| 25 | dc.estupinan170@uniandes.edu.co | | | | | | TRUE | | | | 5a427c85b7 | LinkedIn |
| 26 | anpatin@uniandes.edu.co | | | | | | TRUE | | | | WEnWaSMt | Adobe |

FINAL

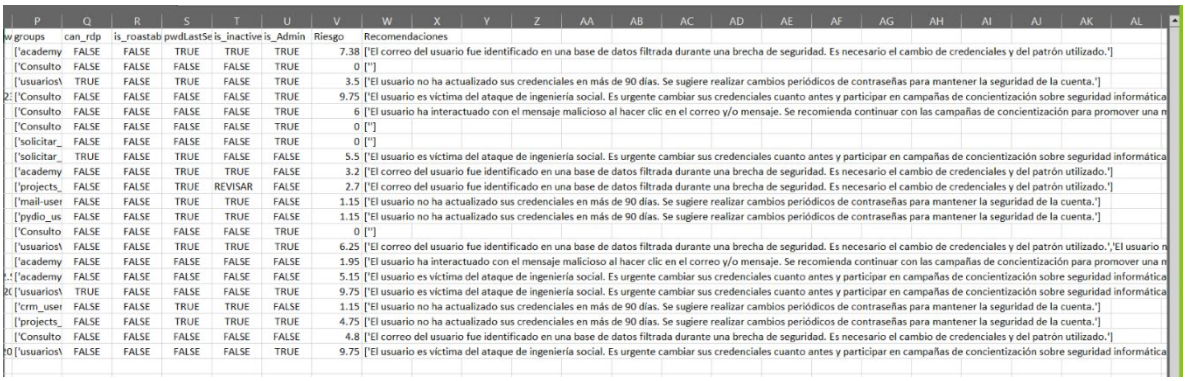
*Figura 5: Archivo resultado modulo OSINT*

**Implementación del Módulo de Phishing.** La aplicación toma la información del archivo generado en el paso anterior, emplea una plantilla de correo predeterminada y realiza el envío de correo tipo phishing:

```
#Users File
data = pd.read_excel('usuarios.xlsx')
#SMTP User
sender_email = "notificaciones0@domainTest.co"
#SMTP Password
password = "Contraseña"
#URL Antes del ID
url = "https://domainTest.co/redirection/redirection.php?id="
#Waiting time between e-mails in seconds
wTime = 60

for i in range(len(data)):
    nombre = data['Nombre'][i]
    receiver_email = data['Correo'][i]
    ids = data['ID'][i]

    urlT = url+ids

    #Email Headers
    msg = MIMEMultipart()
    msg["Subject"] = nombre + ", tu cuenta de OneDrive ha quedado sin espacio."
    msg["From"] = sender_email
    msg["To"] = receiver_email

    #Email Template in HTML file
    file = open('email.html',mode='r',encoding="utf-8")
    html = file.read().format(Nombre=nombre,CORREO=receiver_email,URL='"'+urlT+'"')
    file.close()

    #Attach Headers and Body (Template)
    part = MIMEText(html, "html")
    msg.attach(part)

    #Call SMTP Server
    server = smtplib.SMTP('smtp.dreamhost.com', 587)
    server.login(sender_email, password)
    server.send_message(msg, from_addr=sender_email, to_addrs=receiver_email)

    print("Sent to: " + receiver_email())

    time.sleep(wTime)
```

*Figura 6: Código fuente envío de correo phishing*

**Implementación del Módulo de Riesgo**. La aplicación establece una conexión con el sistema de información del Directorio Activo On premise, para extraer datos como: grupos, rdp, contraseña. Posteriormente, se realiza el cálculo de riesgo. La figura siguiente presenta el resultado luego de hacer el cálculo de riesgo y generar el valor de riesgo y las recomendaciones es:



| P | Q | R | S | T | U | V | W | X | Y | Z | AA | AB | AC | AD | AE | AF | AG | AH | AI | AJ | AK | AL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| w groups | can_rdp | is_roastab | pwdLastSe | is_inactive | is_Admin | Riesgo | Recomendaciones | | | | | | | | | | | | | | | |
| ['academy | FALSE | FALSE | TRUE | TRUE | TRUE | 7.38 | ['El correo del usuario fue identificado en una base de datos filtrada durante una brecha de seguridad. Es necesario el cambio de credenciales y del patrón utilizado.'] | | | | | | | | | | | | | | | |
| ['Consulto | FALSE | FALSE | FALSE | FALSE | TRUE | 0 | ['] | | | | | | | | | | | | | | | |
| ['usuarios\ | TRUE | FALSE | TRUE | FALSE | TRUE | 3.5 | ['El usuario no ha actualizado sus credenciales en más de 90 días. Se sugiere realizar cambios periódicos de contraseñas para mantener la seguridad de la cuenta.'] | | | | | | | | | | | | | | | |
| 2: ['Consulto | FALSE | FALSE | FALSE | FALSE | TRUE | 9.75 | ['El usuario es víctima del ataque de ingeniería social. Es urgente cambiar sus credenciales cuanto antes y participar en campañas de concientización sobre seguridad informática | | | | | | | | | | | | | | | |
| ['Consulto | FALSE | FALSE | FALSE | FALSE | TRUE | 6 | ['El usuario ha interactuado con el mensaje malicioso al hacer clic en el correo y/o mensaje. Se recomienda continuar con las campañas de concientización para promover una n | | | | | | | | | | | | | | | |
| ['Consulto | FALSE | FALSE | FALSE | FALSE | TRUE | 0 | ['] | | | | | | | | | | | | | | | |
| ['solicitar_ | FALSE | FALSE | FALSE | FALSE | TRUE | 0 | ['] | | | | | | | | | | | | | | | |
| ['solicitar_ | TRUE | FALSE | TRUE | FALSE | FALSE | 5.5 | ['El usuario es víctima del ataque de ingeniería social. Es urgente cambiar sus credenciales cuanto antes y participar en campañas de concientización sobre seguridad informática | | | | | | | | | | | | | | | |
| ['academy | FALSE | FALSE | TRUE | TRUE | FALSE | 3.2 | ['El correo del usuario fue identificado en una base de datos filtrada durante una brecha de seguridad. Es necesario el cambio de credenciales y del patrón utilizado.'] | | | | | | | | | | | | | | | |
| ['projects_ | FALSE | FALSE | TRUE | REVISAR | FALSE | 2.7 | ['El correo del usuario fue identificado en una base de datos filtrada durante una brecha de seguridad. Es necesario el cambio de credenciales y del patrón utilizado.'] | | | | | | | | | | | | | | | |
| ['mail-user | FALSE | FALSE | TRUE | TRUE | FALSE | 1.15 | ['El usuario no ha actualizado sus credenciales en más de 90 días. Se sugiere realizar cambios periódicos de contraseñas para mantener la seguridad de la cuenta.'] | | | | | | | | | | | | | | | |
| ['pydio_us | FALSE | FALSE | TRUE | TRUE | FALSE | 1.15 | ['El usuario no ha actualizado sus credenciales en más de 90 días. Se sugiere realizar cambios periódicos de contraseñas para mantener la seguridad de la cuenta.'] | | | | | | | | | | | | | | | |
| ['Consulto | FALSE | FALSE | FALSE | FALSE | TRUE | 0 | ['] | | | | | | | | | | | | | | | |
| ['usuarios\ | FALSE | FALSE | TRUE | TRUE | TRUE | 6.25 | ['El correo del usuario fue identificado en una base de datos filtrada durante una brecha de seguridad. Es necesario el cambio de credenciales y del patrón utilizado.','El usuario n | | | | | | | | | | | | | | | |
| ['academy | FALSE | FALSE | FALSE | FALSE | FALSE | 1.95 | ['El usuario ha interactuado con el mensaje malicioso al hacer clic en el correo y/o mensaje. Se recomienda continuar con las campañas de concientización para promover una n | | | | | | | | | | | | | | | |
| ['academy | FALSE | FALSE | FALSE | FALSE | FALSE | 5.15 | ['El usuario es víctima del ataque de ingeniería social. Es urgente cambiar sus credenciales cuanto antes y participar en campañas de concientización sobre seguridad informática | | | | | | | | | | | | | | | |
| 2( ['usuarios\ | TRUE | FALSE | FALSE | FALSE | TRUE | 9.75 | ['El usuario es víctima del ataque de ingeniería social. Es urgente cambiar sus credenciales cuanto antes y participar en campañas de concientización sobre seguridad informática | | | | | | | | | | | | | | | |
| ['crm_user | FALSE | FALSE | TRUE | TRUE | FALSE | 1.15 | ['El usuario no ha actualizado sus credenciales en más de 90 días. Se sugiere realizar cambios periódicos de contraseñas para mantener la seguridad de la cuenta.'] | | | | | | | | | | | | | | | |
| ['projects_ | FALSE | FALSE | TRUE | TRUE | TRUE | 4.75 | ['El usuario no ha actualizado sus credenciales en más de 90 días. Se sugiere realizar cambios periódicos de contraseñas para mantener la seguridad de la cuenta.'] | | | | | | | | | | | | | | | |
| ['Consulto | FALSE | FALSE | FALSE | FALSE | FALSE | 4.8 | ['El correo del usuario fue identificado en una base de datos filtrada durante una brecha de seguridad. Es necesario el cambio de credenciales y del patrón utilizado.'] | | | | | | | | | | | | | | | |
| 0 ['usuarios\ | FALSE | FALSE | FALSE | FALSE | TRUE | 9.75 | ['El usuario es víctima del ataque de ingeniería social. Es urgente cambiar sus credenciales cuanto antes y participar en campañas de concientización sobre seguridad informática | | | | | | | | | | | | | | | |

*Figura 7: Archivo resultado del cálculo de riesgo*

Estas recomendaciones se generan con base en la valoración de riesgo y las características detectadas en la cuenta de usuario. Cada recomendación tiene asignado un identificador interno que luego se utiliza para obtener estadísticas y generar métricas. Al igual que en un proyecto de Ethical Hacking, estas recomendaciones se generan principalmente utilizando el conocimiento y la experiencia del equipo de profesionales de seguridad involucrado en el proyecto. Estos expertos poseen un amplio conocimiento técnico en áreas como Pentesting a Directorio Activo, Ingeniería Social, Infraestructura, entre otros. Para asegurar la efectividad de las recomendaciones, estas se basan en las mejores prácticas y estándares de seguridad reconocidos, como el OSSTMM (Open Source Security Testing Methodology Manual), el NIST (National Institute of Standards and Technology), el CIS (Center for Internet Security), entre otros.

## 4. Conclusiones y Trabajo Futuro

Se logró la extracción de información de las diferentes fuentes OSINT integradas en el proceso, dando como resultado la información básica para poder ejecutar el siguiente paso que es enviar el correo al listado obtenidos por el módulo OSINT, si bien no se probó la posibilidad de construir una plantilla con base en la información colectada, se espera que en versiones posteriores se pueda integrar esta funcionalidad a través por ejemplo de IA que ayude en la automatización de este paso y sea transparente la construcción de la plantilla o pretexto para el correo objetivo.

También se logró probar el módulo de análisis de riesgo, el factor diferenciador de este software frente al resto de herramientas que existen en el mercado de simulación de ingeniería social, dando como resultado, una medición de riesgo con base en los privilegios, accesos, rol y el resultado de las fuentes OSINT. Igualmente se presentan unas recomendaciones que pudieran considerar para minimizar la probabilidad de materialización de un incidente de seguridad de la información.

Se confía que esta herramienta se convierta en un recurso fundamental (como lo son en este momento una herramienta de detección de malware y anomalías o una herramienta de seguridad perimetral) para las compañías a la hora de realizar campañas de sensibilización.

Como trabajo futuro, pensamos que con el apoyo de Inteligencia Artificial esta herramienta de phishing puede integrar técnicas de aprendizaje automático para crear mensajes de correo electrónico más convincentes y personalizados que persuadan a las víctimas a hacer clic en enlaces maliciosos o proporcionen información confidencial. Adicionalmente, utilizando redes sociales y en general la información en internet, se puede utilizar técnicas de análisis de datos y aprendizaje automático para identificar patrones de comportamiento y preferencias de los usuarios y utilizar esa información para adaptar mensajes de marketing a personas individuales.

El alcance inicial de este software incluye la integración con Directorio Activo on premise, pero se espera evolucionar e integrarse con el Directorio Activo en la nube y con otras clases de sistemas de información que puedan ofrecer beneficios complementarios para lograr enriquecer aún más el perfil de riesgo y ser más precisos a la hora de medirlo. Por ejemplo: SIEM, sistemas de información de gestión remota de acceso como Citrix, etc.

## 5. Referencias


[1] "Arma Infalible - Ingeniería Social", en Academia.edu, [En línea]. Disponible en: https://www.academia.edu/download/55136701/Arma_Infalible_-_Ingenieria_Social.pdf. Accedido: 20 de mayo 2023.

[2] Segu-Info. "Ingeniería Social". Segu-Info [En línea]. Disponible en: https://www.segu-info.com.ar/articulos/30-ingenieria-social. Accedido en: 20 de mayo 2023.

[3] Entelgy. "La persona es el eslabón más débil de la cadena". Entelgy Digital. 22 de mayo de 2019. Disponible en: https://www.entelgy.com/divisiones/digital/actualidad-digital/digital/noticias-corporativas-digital/la-persona-es-el-eslabon-mas-debil-de-la-cadena. Accedido en: 24 de abril de 2023.

[4] Verizon. (2022). 2022 Data Breach Investigations Report (DBIR). [Online]. Disponible en: https://www.verizon.com/business/resources/T7fa/reports/dbir/2022-data-breach-investigations-report-dbir.pdf [Consultado en fecha: 21 de mayo de 2023.].

[5] Read the Docs. "LDAP3 Tutorial Introduction". Read the Docs [En línea]. Disponible en: https://ldap3.readthedocs.io/en/latest/tutorial_intro.html. Accedido en: 21 de mayo de 2023.

[6] PyPI. "pandas". PyPI [En línea]. Disponible en: https://pypi.org/project/pandas/. Accedido en: 21 de mayo de 2023.

[7] Netwrix Blog. "CrackMapExec Tutorial". Netwrix Blog [En línea]. Disponible en: https://blog.netwrix.com/2022/12/16/crackmapexec_tutorial/. Accedido en: 27 de abril de 2023.