**Ingeniería Social**

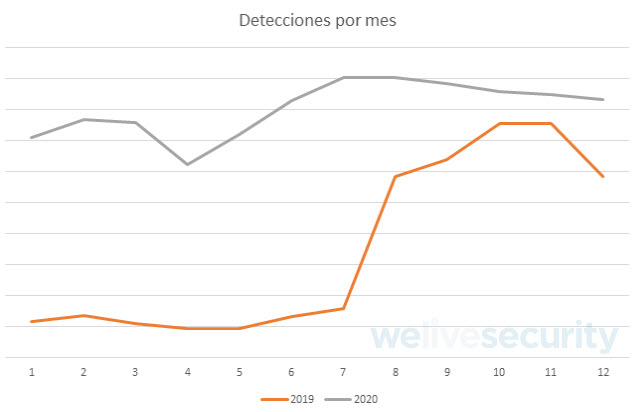
Actualmente está creciendo el nivel de protección tanto en seguridad local como en seguridad en red utilizando herramientas tanto hardware como software además de otros medios. Por ello se están incrementando los ataques basados en ingeniería social contra el elemento más débil de un sistema informático, el ser humano. Estos ataques básicamente consisten en conseguir que una persona realice una acción que provoque una brecha de seguridad que por medios naturales no haría. La mejor solución frente a estos ataques es la formación, de las personas, acerca de cómo se producen.

**Ejercicios:**

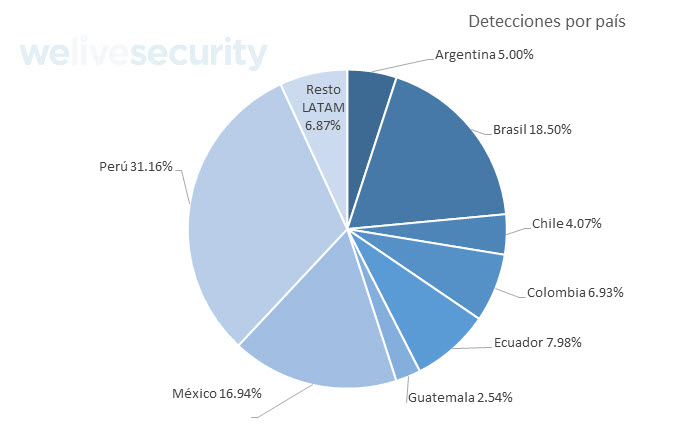
• Busca varias definiciones sobre ingeniería social aplicadas al campo de la seguridad informática:

* Es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.
* Es una de las formas en las que los cibercriminales usan las interacciones entre personas para que el usuario comparta información confidencial. Ya que la ingeniería social se basa en la naturaleza humana y las reacciones humanas, hay muchas formas en que los atacantes pueden engañar, en línea o sin conexión.
* El término ingeniería social tiene su origen en las ciencias sociales, donde se refiere a cualquier esfuerzo de los factores de cambio (por ejemplo, medios de comunicación, gobiernos o grupos privados) con el propósito de influir o moldear el comportamiento de la población objetivo. En términos más simples, la ingeniería social implica el uso de la manipulación con el fin de conseguir un fin, ya sea bueno (por ejemplo, promover la tolerancia) o malo (por ejemplo, el belicismo). Aunque se remonta al siglo XIX, el término ingeniería social hoy se asocia mayoritariamente con la ciberseguridad.

• Busca estadísticas sobre el porcentaje de ataques basados en ingeniería social:









El primer paso para realizar un ataque basado en ingeniería social es la obtención de información. Cuanta mayor información se posea acerca del objetivo más fácil resultará realizar posteriormente el ataque. En el caso de una empresa está información va desde software empleado, formas de contacto, proveedores de servicios, estructura de los departamentos, aficiones de los empleados, etc...

Para obtener está información existen 4 métodos:

• Obtención directa

• Información pública (ej. página web, redes sociales...)

• Comprar la información a un proveedor de este servicio.

• Ataque para obtener información

Tener mucha información es tan importante como organizarla y analizarla para después poder emplearla en un ataque. Existen programas tipo “bloc de notas” que permiten incluir más información que sólo texto y jerarquizarla. Unos ejemplos serían: Basket Note Pads, KeepNote o Dradis.

**Ejercicios:**

• Utilizando uno de estos programas reunir información limpiamente (mediante fuentes libres/públicas) acerca de un personaje famoso o una empresa conocida:



El segundo paso es utilizar esa información para, mediante un engaño, conseguir que alguien revele información o realice alguna acción que ponga en jaque la seguridad de un sistema. Aquí es donde entran en juego las habilidades de ingeniería social como tal, en la manipulación de las personas. En el apartado anterior depende de cómo se obtenga la información puede ser legal o ilegal. En este apartado la mayoría de los casos son considerados ilegales.

**Ejercicios:**

• Buscar fragmentos de películas donde a través de un engaño (falsa identidad, suplantación de identidad, …) el atacante consiga entrar en las oficinas de alguna empresa.

<https://youtu.be/QMG_GeI90rI>

• Definir los siguientes vectores de ataque:

* **Phishing:** es un método para engañar a una persona y hacer que comparta contraseñas, números de tarjeta de crédito, y otra información confidencial haciéndose pasar por una institución de confianza en un mensaje de correo electrónico o llamada telefónica.
* **Vishing:** un tipo de ataque peligrosamente eficaz que se apoya en técnicas de ingeniería social y en el cual el atacante se comunica telefónicamente o vía mensaje de voz haciéndose pasar por una empresa o entidad confiable con la intención de engañar a la víctima y convencerla de que realice una acción que va en contra de sus intereses.
* **Impersonation:** es una forma de fraude en la que los atacantes se hacen pasar por una persona conocida o de confianza para engañar a un empleado para que transfiera dinero a una cuenta fraudulenta, comparta información confidencial (como propiedad intelectual, datos financieros o información de nómina) o revele las credenciales de inicio de sesión. que los atacantes pueden usar para piratear la red informática de una empresa. El fraude del CEO, el compromiso del correo electrónico comercial y la caza de ballenas son formas específicas de ataques de suplantación de identidad en los que personas malintencionadas se hacen pasar por ejecutivos de alto nivel dentro de una empresa.
* **SMiShing:** s una técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima -red social, banco, institución pública, etc. -con el objetivo de robarle información privada o realizarle un cargo económico. Generalmente el mensaje invita a llamar a un número de tarificación especial o acceder a un enlace de una web falsa bajo un pretexto.

El último paso, conseguido ya el ataque de ingeniería social, es propiamente el ataque informático. Consiste en utilizar herramientas de “exploit o metaexploit” para utilizando una vulnerabilidad del sistema perpetrar el ataque. Estas herramientas se pueden encontrar en distribuciones de Linux como Kali Linux (antiguamente conocido como BackTrack Linux). La aparición de las mismas es para emplearlas en auditorias de seguridad informática y poner a prueba la seguridad de una empresa. En ningún caso deben utilizarse en un ataque real.

**Ejercicios:**

• Enfoque práctico con Kali Linux:

<http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf>

**4. CAPTURAR INFORMACIÓN:**

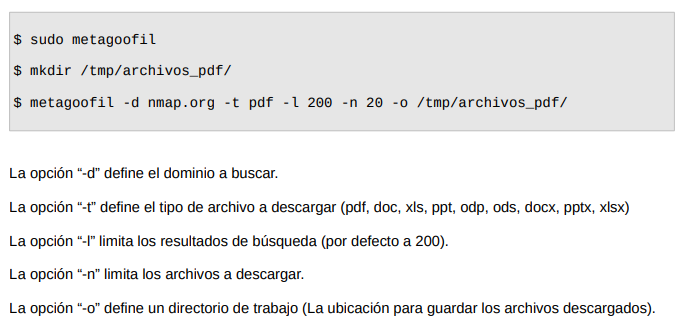
En esta fase se intenta recolectar la mayor cantidad de información posible sobre el objetivo en evaluación, como posibles nombres de usuarios, direcciones IP, servidores de nombre, y otra información relevante.

El proceso donde se captura la información puede ser dividido de dos maneras. La captura de información activa y la captura de información pasiva. En el primera forma se recolecta información enviando tráfico hacia la red objetivo, como por ejemplo realizar ping ICMP, y escaneos de puertos TCP/UDP. Para el segundo caso se obtiene información sobre la red objetivo utilizando servicios o fuentes de terceros, como por ejemplo motores de búsqueda como Google y Bing, o utilizando redes sociales como Facebook o LinkedIn.

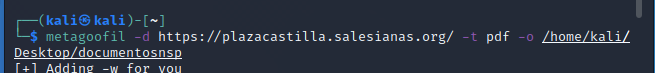
**Capturar documentos:**

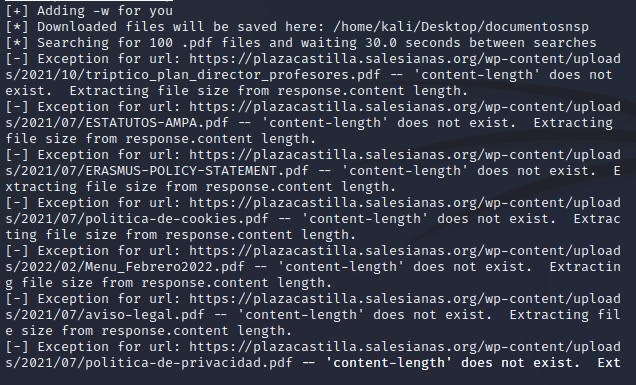
* **Metagoofil:** es una herramienta diseñada par capturar información mediante la extracción de metadatos desde documentos públicos (pdf, doc, xls, ppt, odp, ods, docx, pptx, xlsx) correspondientes a la organización objetivo.

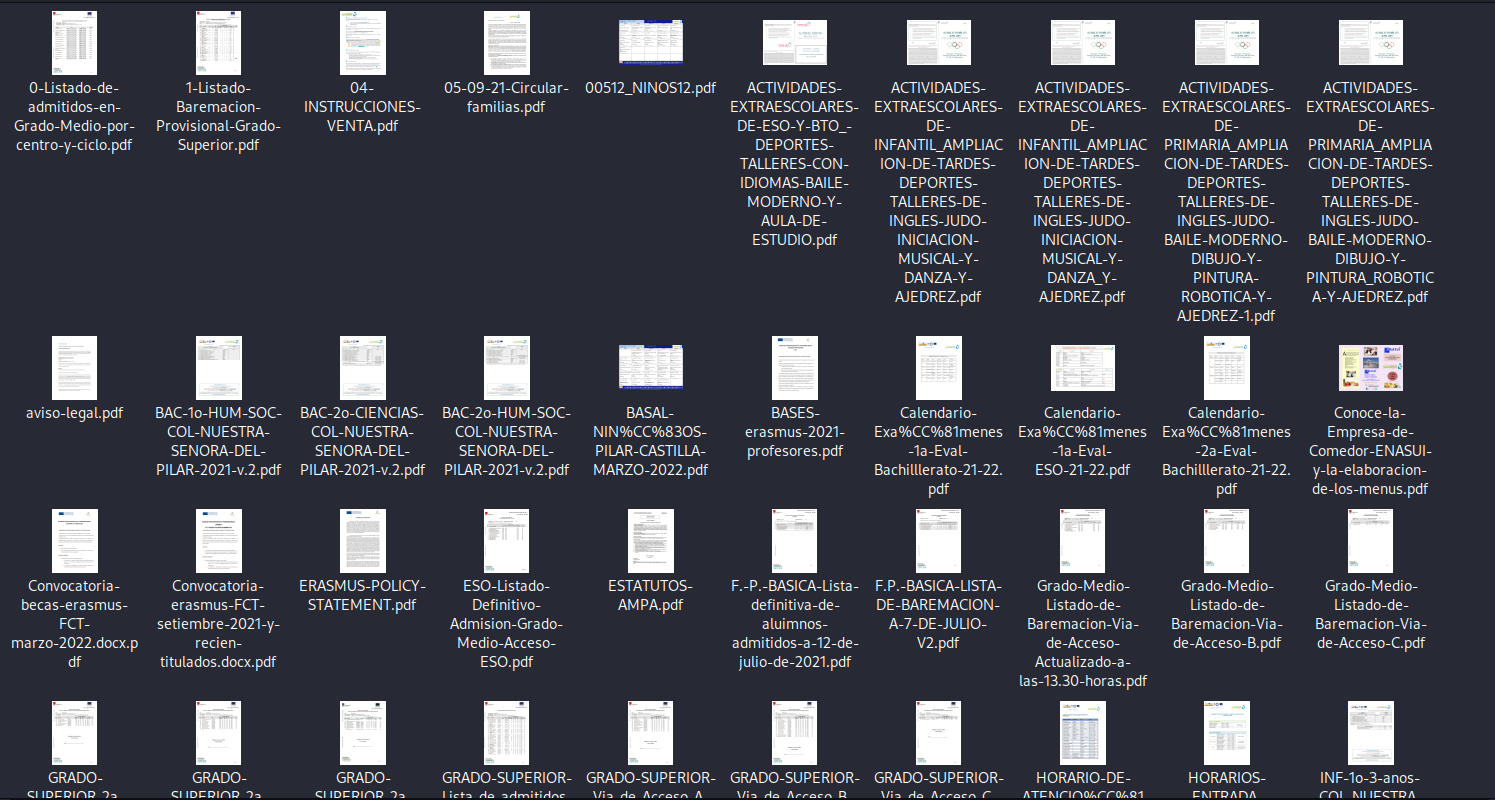
Metagoofil realizará una búsqueda en Google para identificar y descargar documentos hacia el disco local, y luego extraerá los metadatos con diferentes librerías como Hachoir, PdfMiner y otros. Con los resultados se generará un reporte con los nombres de usuarios, versiones y software, y servidores o nombres de las máquinas, las cuales ayudarán a los profesionales en pruebas de penetración en la fase para la captura de información.



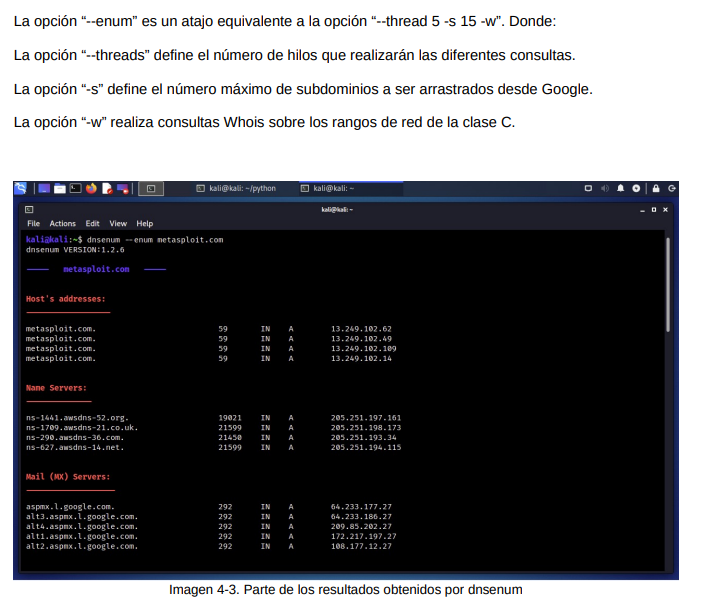
* Instalación:
  + sudo apt-get update
  + sudo apt-get install metagoofil

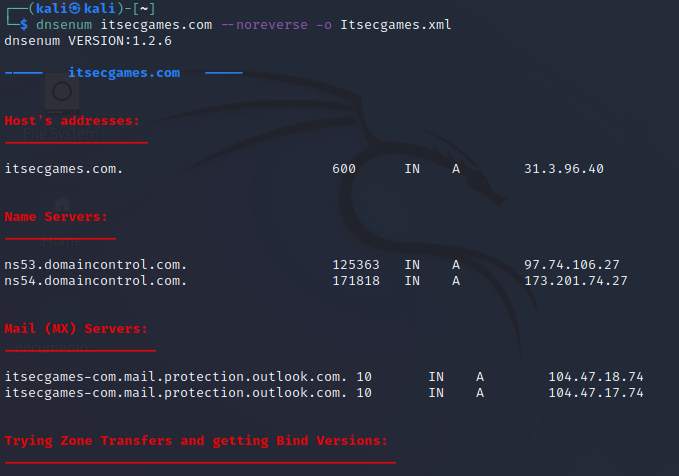






* **DNSenum:** El propósito de DNSenum es capturar tanta información como sea posible sobre un dominio. Realizando actualmente las siguientes operaciones:
  + Obtener las direcciones IP del host (Registro A).
  + Obtener los servidores de nombres. Obtener el registro MX.
  + Realizar consultas AXFR sobre servidores de nombres y versiones de BIND.
  + Obtener nombres adicionales y subdominios mediante Google (“allinurl -www site:dominio”).
  + Fuerza bruta a subdominios de un archivo, puede también realizar recursividad sobre subdominios los cuales tengan registros NS. Calcular los rangos de red de dominios en clase y realizar consultas whois sobre ellos. Realizar consultas inversas sobre rangos de red (clase C y/o rangos de red).
  + Escribir hacia un archivo domain\_ips.txt los bloques IP
* Instalación sudo apt-get install dnsenum

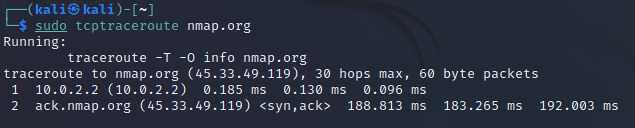




 pg23

**Información de la Ruta:**

* **Tcptraceroute:** es una implementación de la herramienta traceroute, la cual utiliza paquetes TCP para trazar la ruta hacia el host objetivo. Traceroute tradicionalmente envía ya sea paquetes UDP o paquetes ICMP ECHO con un TTL a uno, e incrementa el TTL hasta el destino alcanzado



**Utilizar un motor de búsqueda:**

* **theHarvester:** theHarvester es una herramientas para obtener nombres de dominio, direcciones de correo electrónico, hosts virtuales, banners de puertos abiertos, y nombres de empleados desde diferentes fuentes públicas (motores de búsqueda, servidores de llaves pgp). Las fuentes son; Treatcrowd, crtsh, google, googleCSW, google-profiles, bing, bingapi, dogpile, pgp, linkein, vhost, twitter, googleplus, yahoo, baidu, y shodan.

