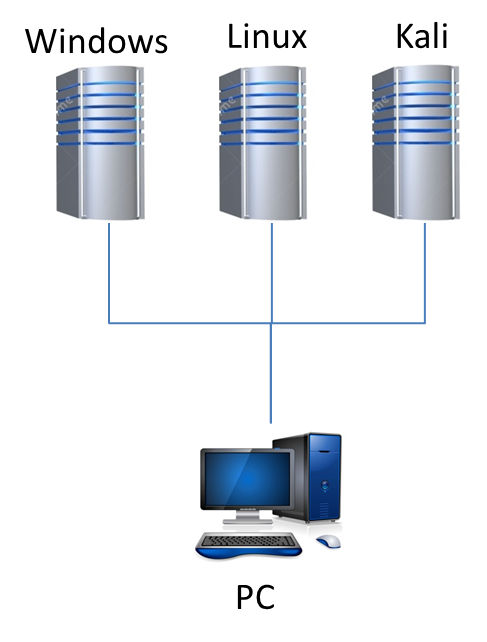
**OBJETIVO:**

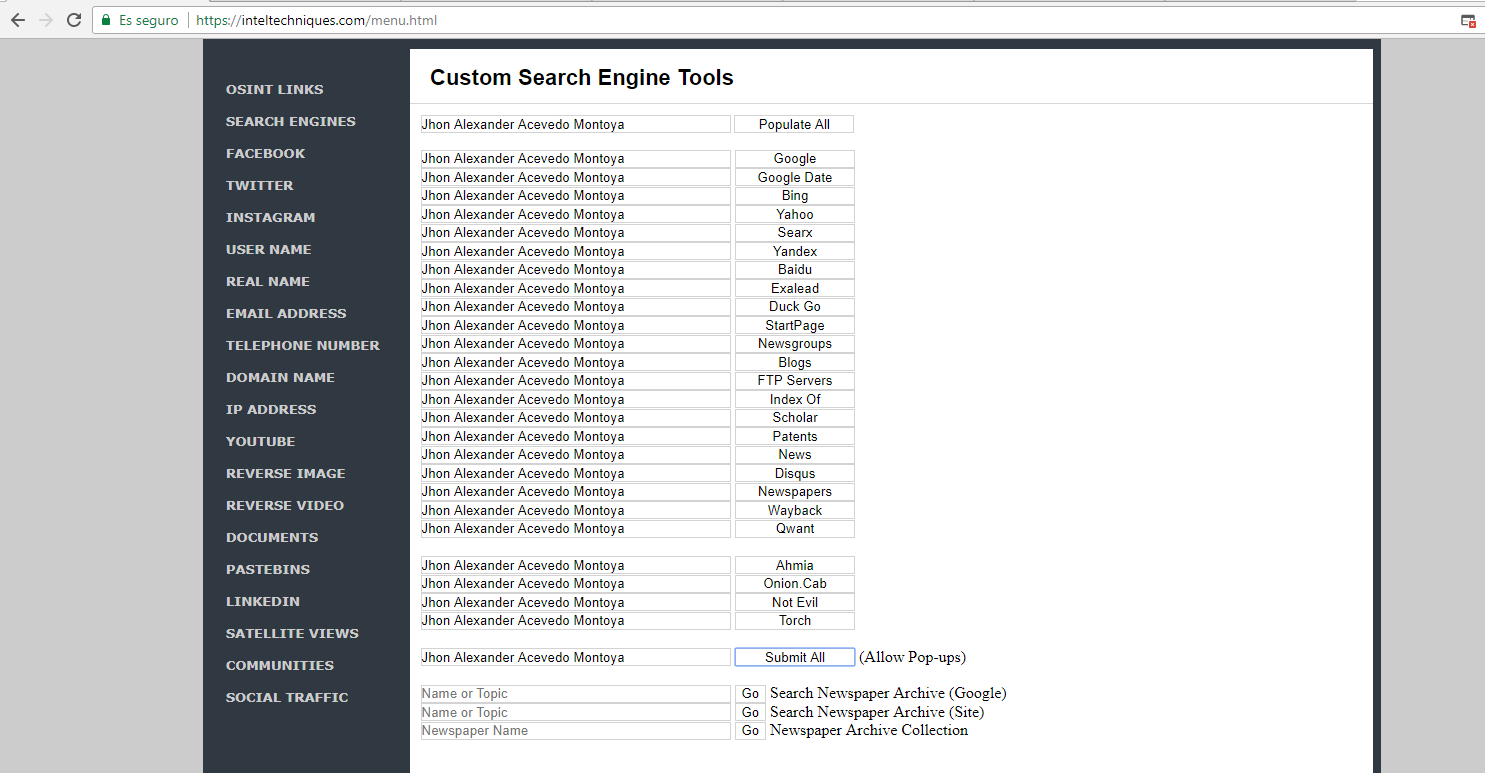
* Comprender el uso de algunas herramientas para gestión de vulnerabilidades.
* Reconocer los datos y resultados del análisis de vulnerabilidades.

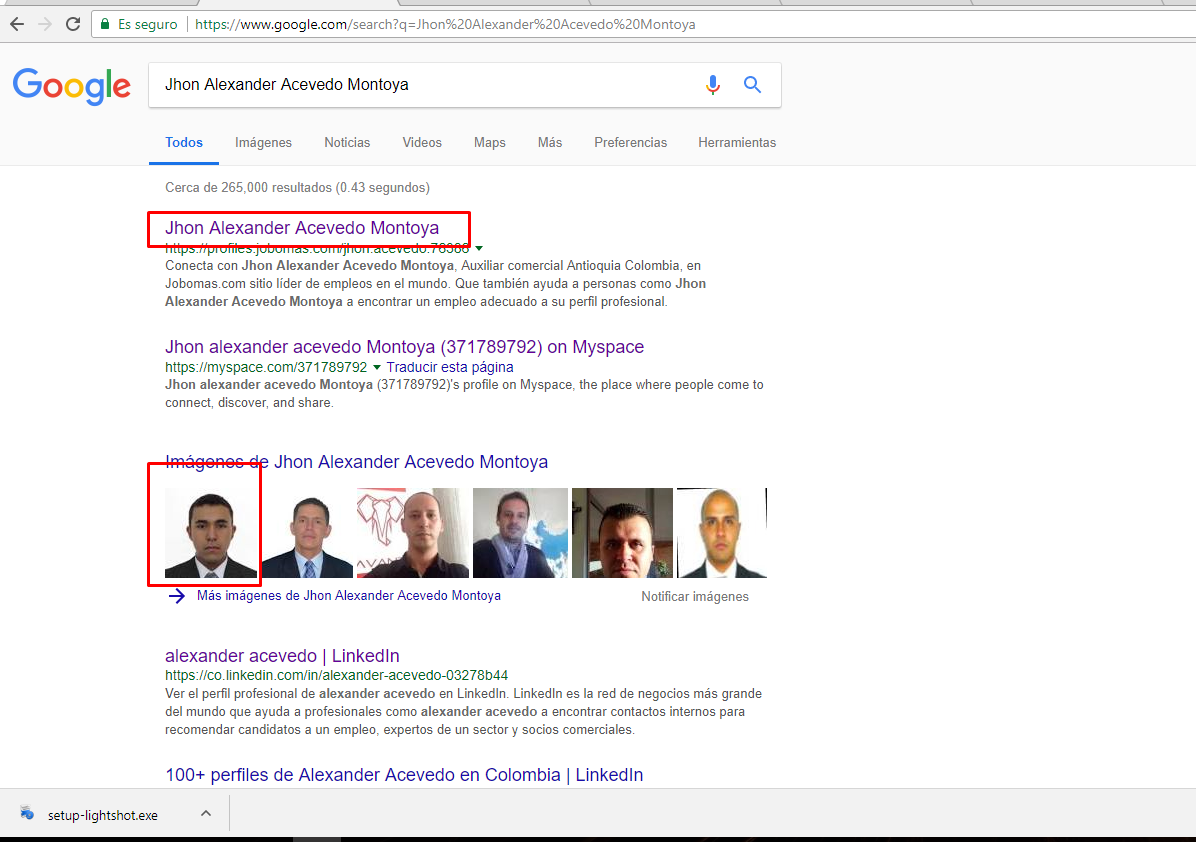
**ESCENARIO**

****

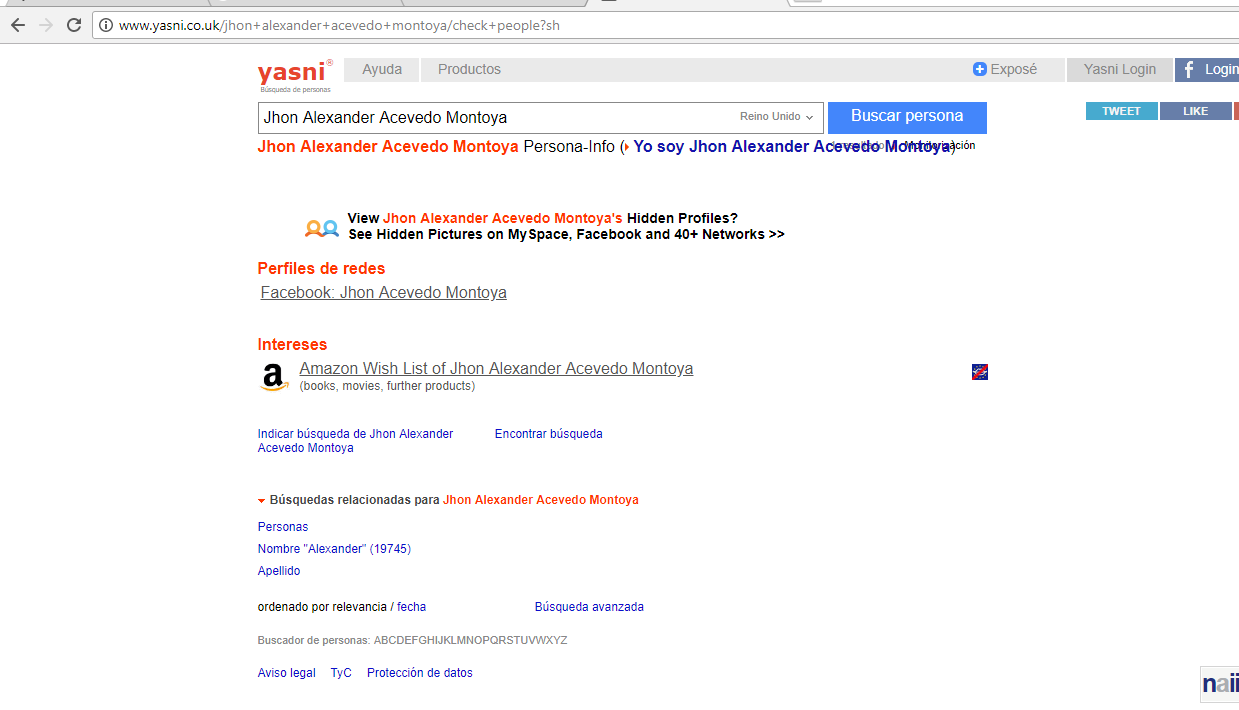
**PROCEDIMIENTO**

1. **PARTE 1 – Técnicas de enumeración**
2. **Fuentes abiertas y buscador de personas**
   1. Haga uso del siguiente enlace para encontrar información de una persona, un concepto o cualquier cosa: <https://inteltechniques.com/menu.html>



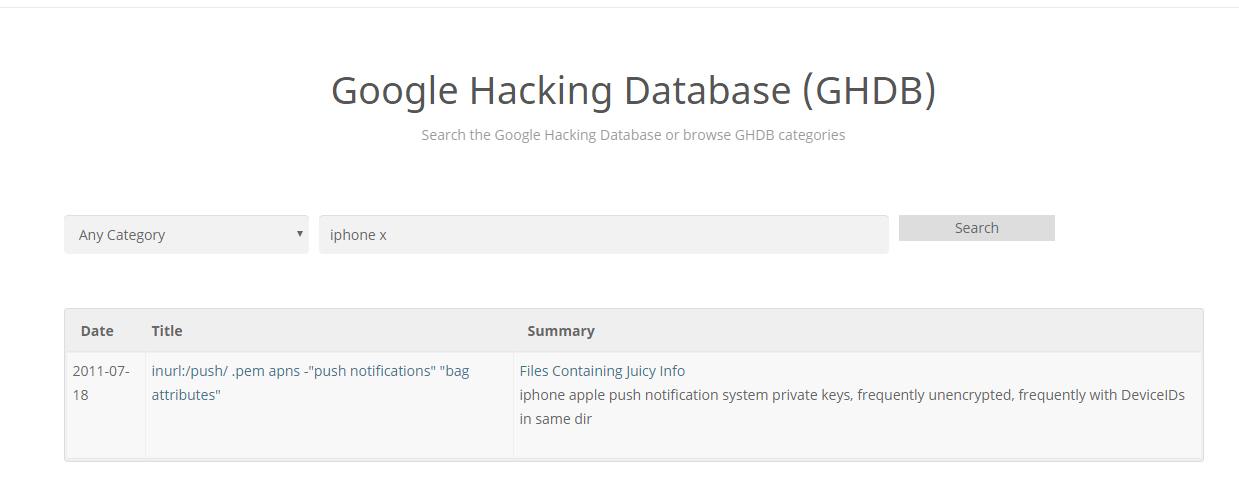


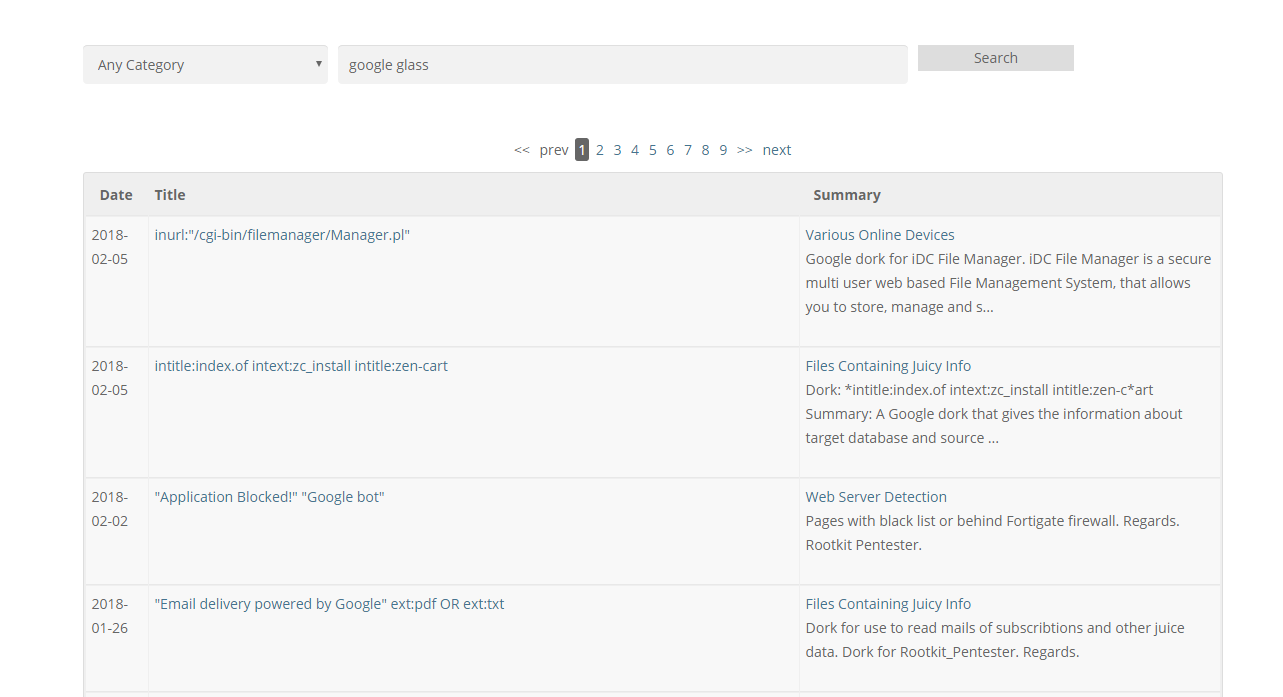


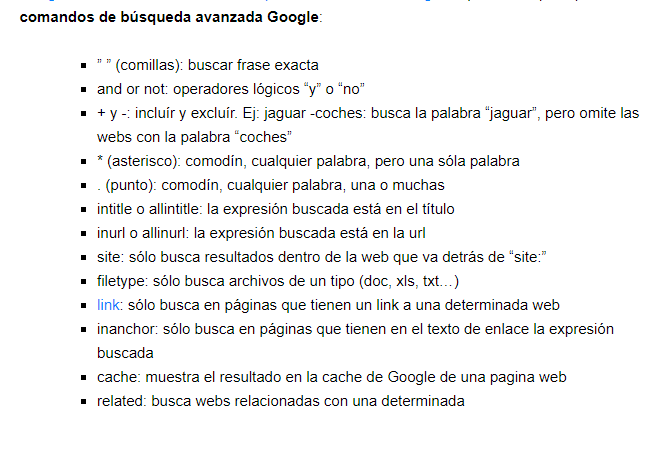
* 1. Ingrese a la URL https://pipl.com/ o [www.yasni.co.uk](http://www.yasni.co.uk) y ejecute una búsqueda de personas.
  2. 
  3. Una vez ingrese los datos, revise los resultados y haga un análisis de la información suministrada. ¿Qué se puede concluir con respecto a la seguridad?

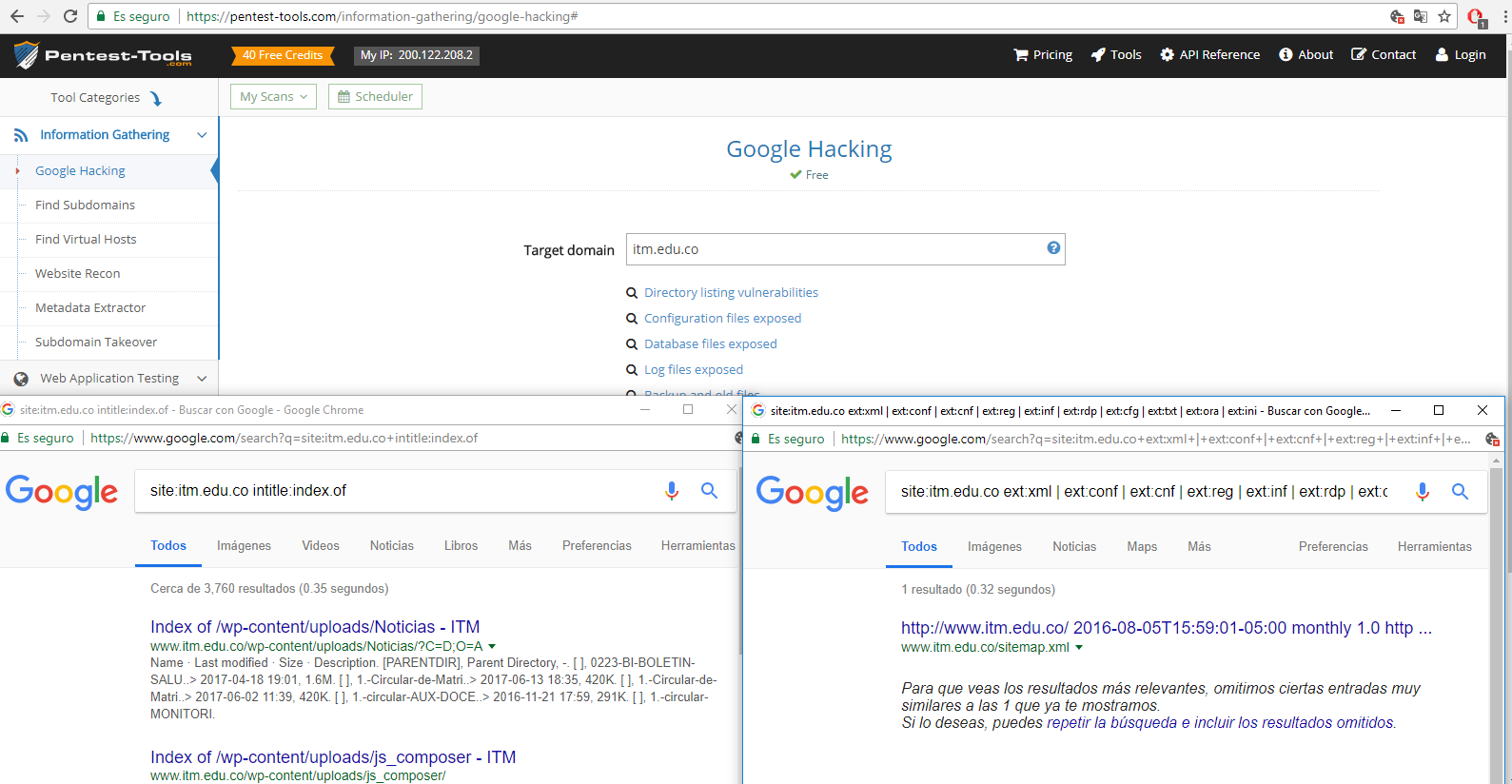
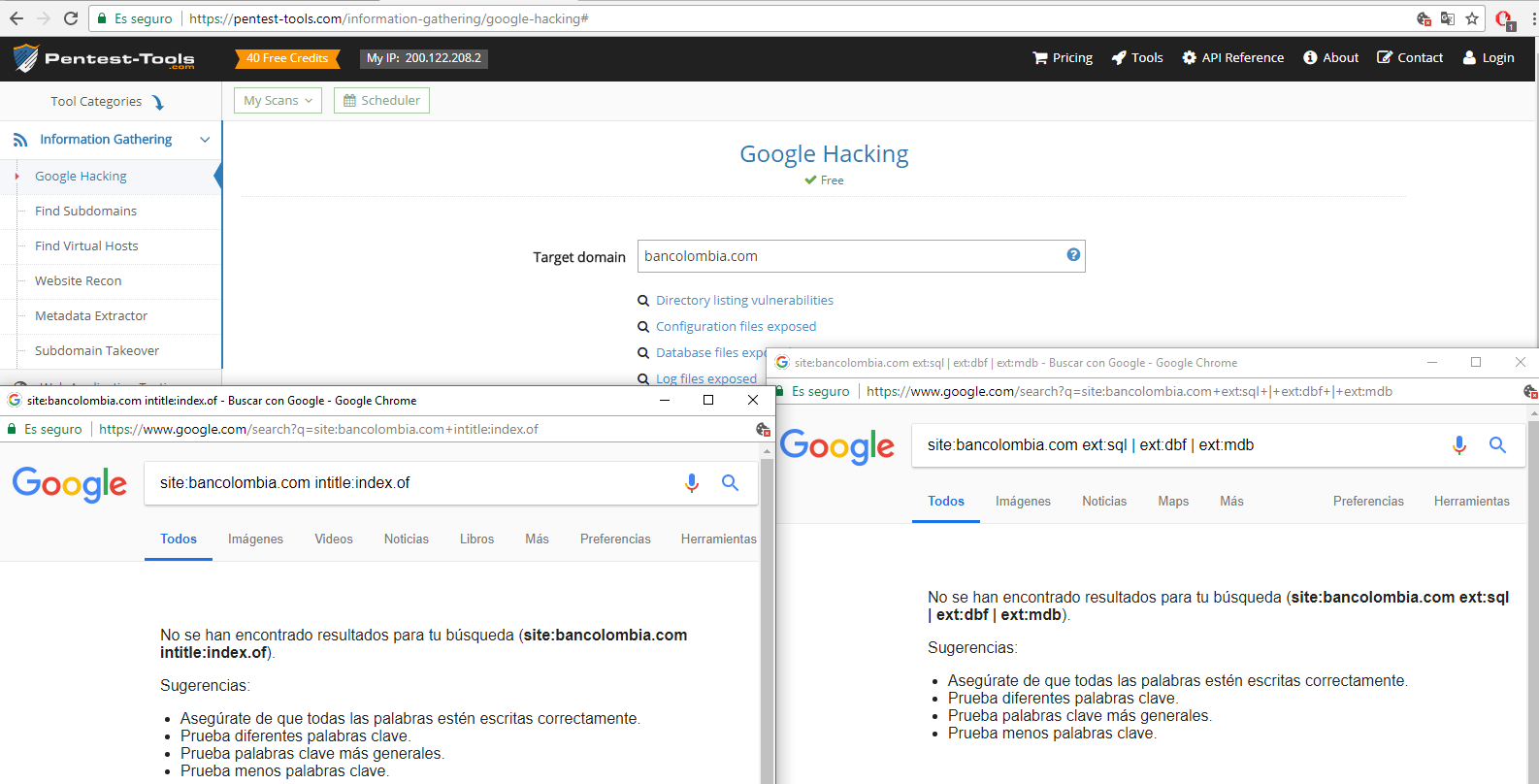
Acerca de la primera búsqueda notamos que encontró al usuario sin problemas en cambio la segunda no arrojo respuestas, lo que nos da entender es que las redes sociales y en este caso paginas de empleo son una fuente de búsqueda más pública y la mayoría de las personas poseen unas

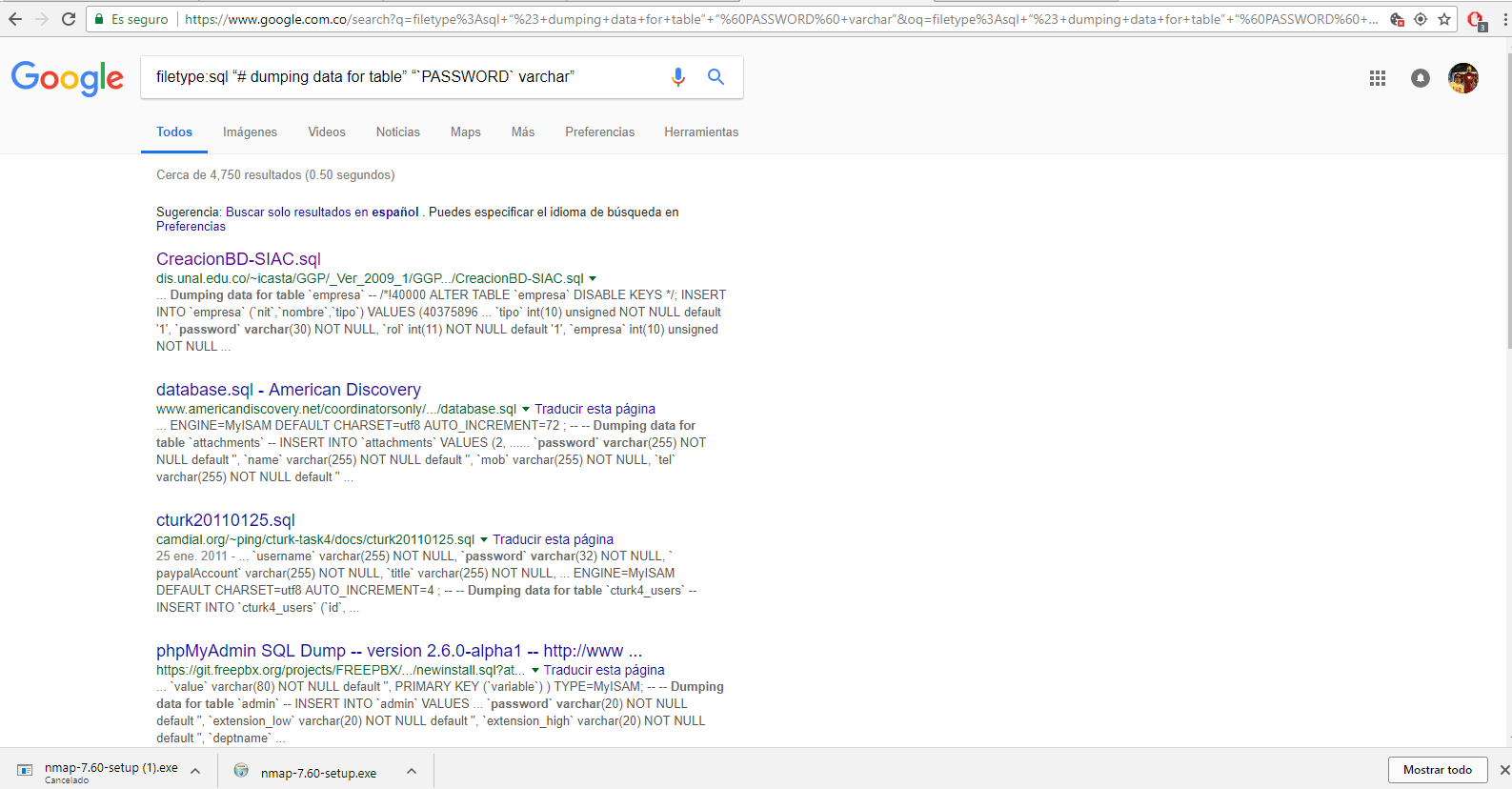
1. Uso de técnicas avanzadas de búsquedas o google hacking
   1. Ingrese al sitio <https://www.exploit-db.com/google-hacking-database/> y busque diferentes elementos tecnológicos como contraseñas, servicios expuestos, cámaras Web abiertas, etc.

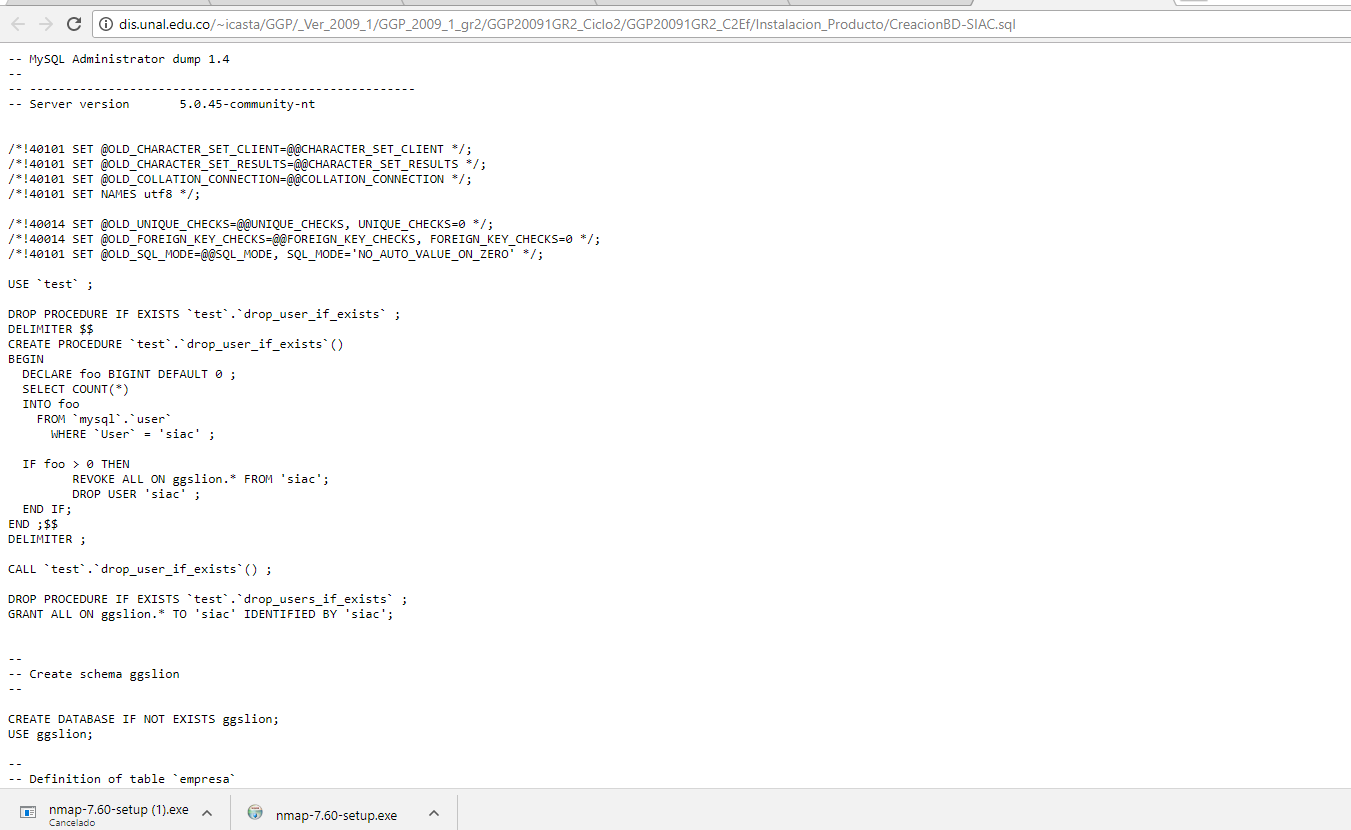


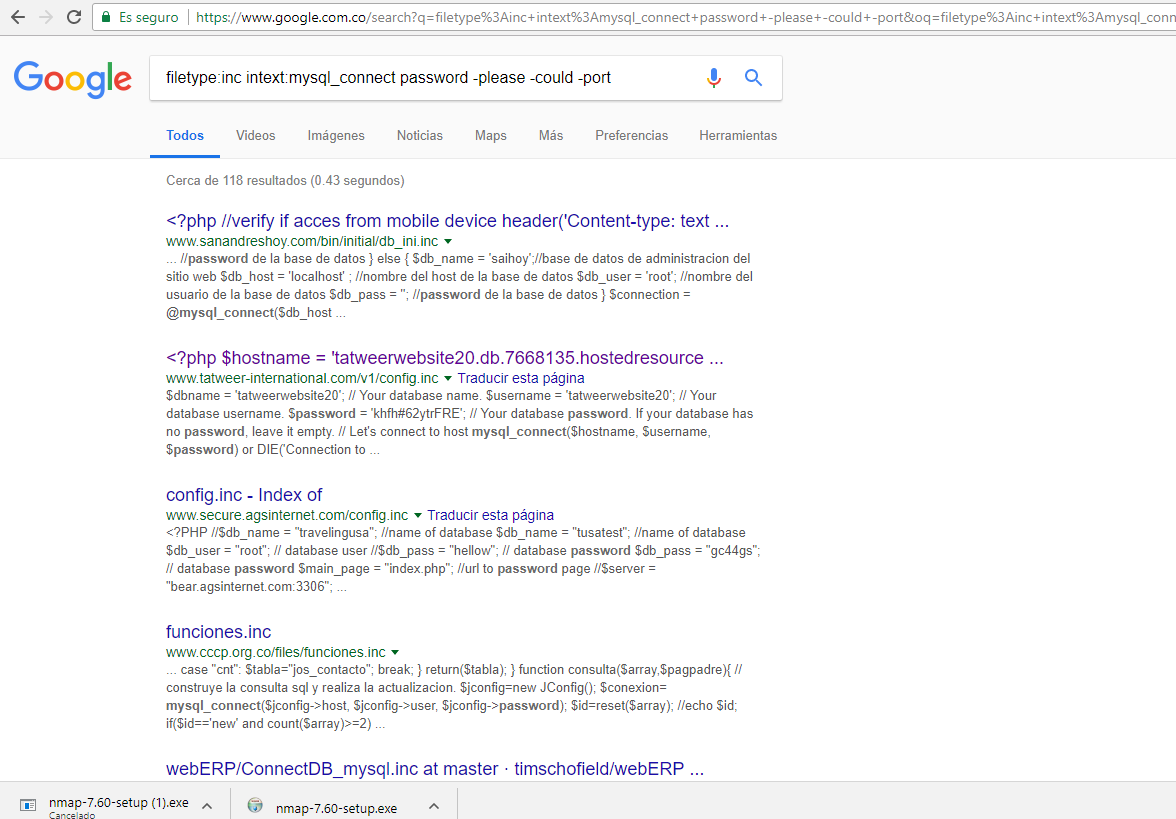


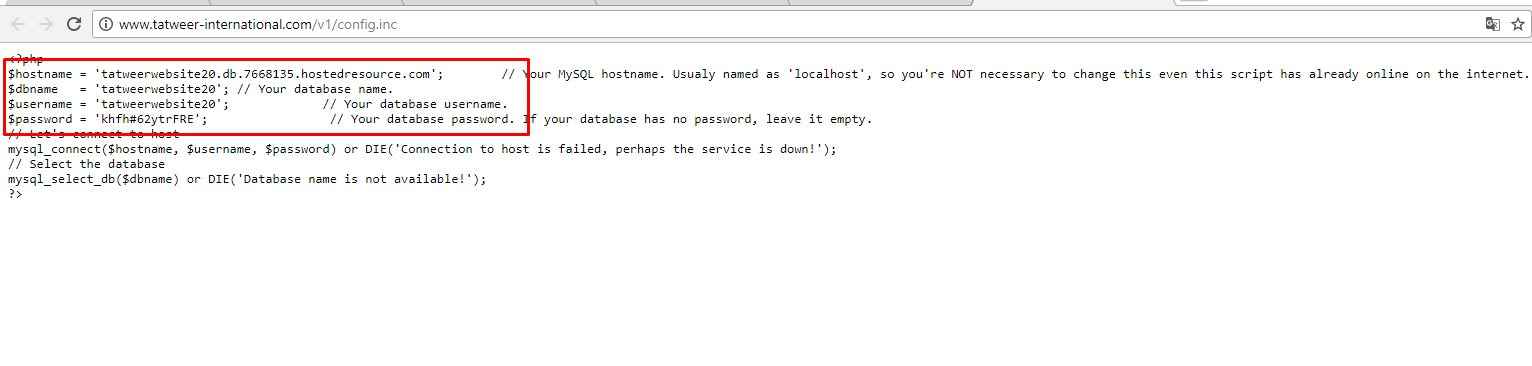


* 1. Busque en internet otro sitio en dónde se pueda referenciar comandos de google hacking.
  2. 
  3. 
  4. Realizamos búsqueda avanzada y encontramos archivos .sql

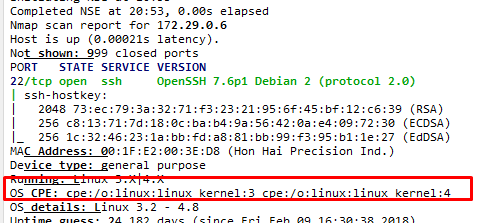




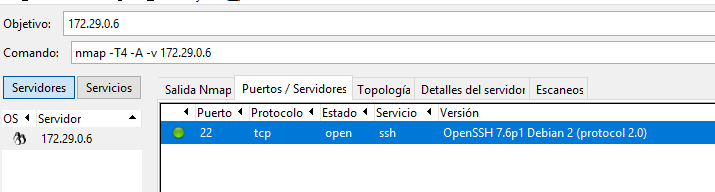




1. **PARTE 2 – Uso de nmap**
2. Instale nmap en Windows, baje el software del servidor Ubuntu hacia el equipo local. **\_ok**
3. Una vez instalado, abre nmap en Windows y ejecuta un escaneo de puertos hacia cualquiera de los servidores Linux, revise cada uno de los resultados e indique que información ha obtenido.

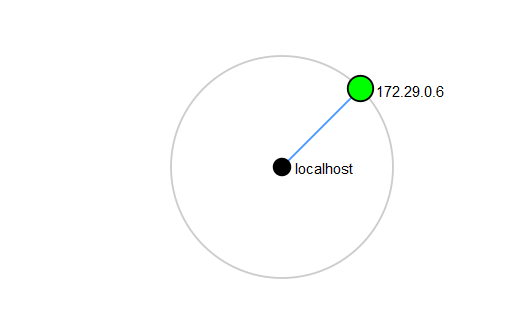


Obtenemos en este escaneo el sistema operativo

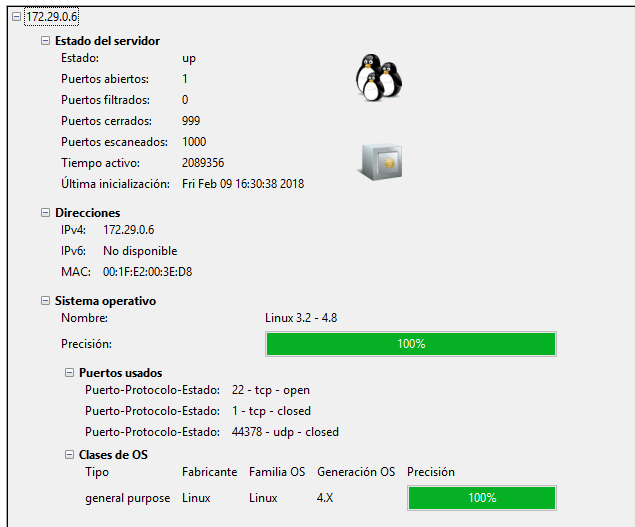


Este escaneo nos arrojo que tiene solo un puerto abierto

Puerto 22 : permite realizar comunicaciones cifradas a través de una red.

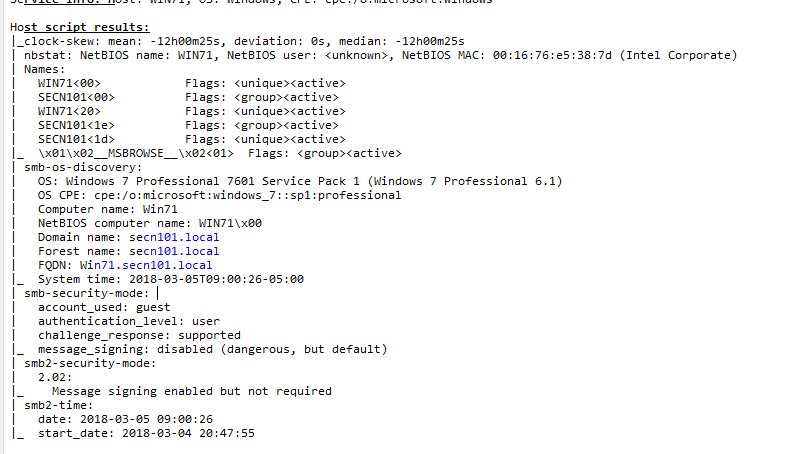


Nos arroja las maquinas que intervinieron a la comunicación del local y el servidor Linux

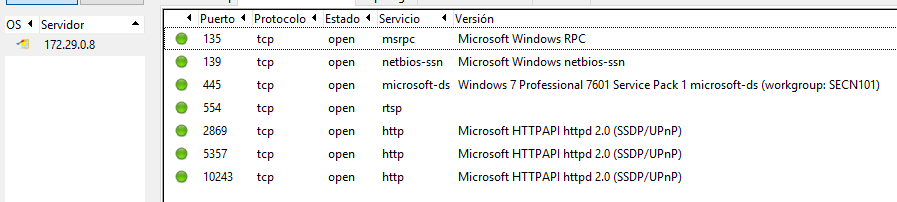


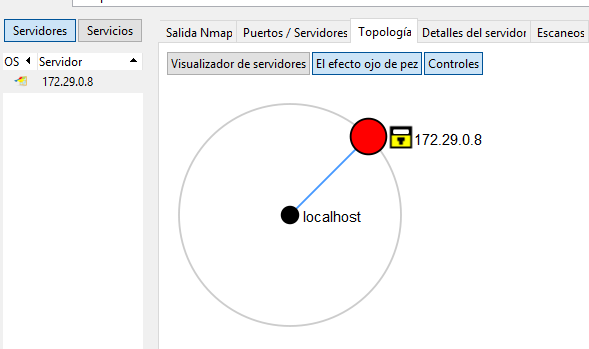
Tenemos mas detalle acerca de los puertos cerrados y el detalle del sistema operativo

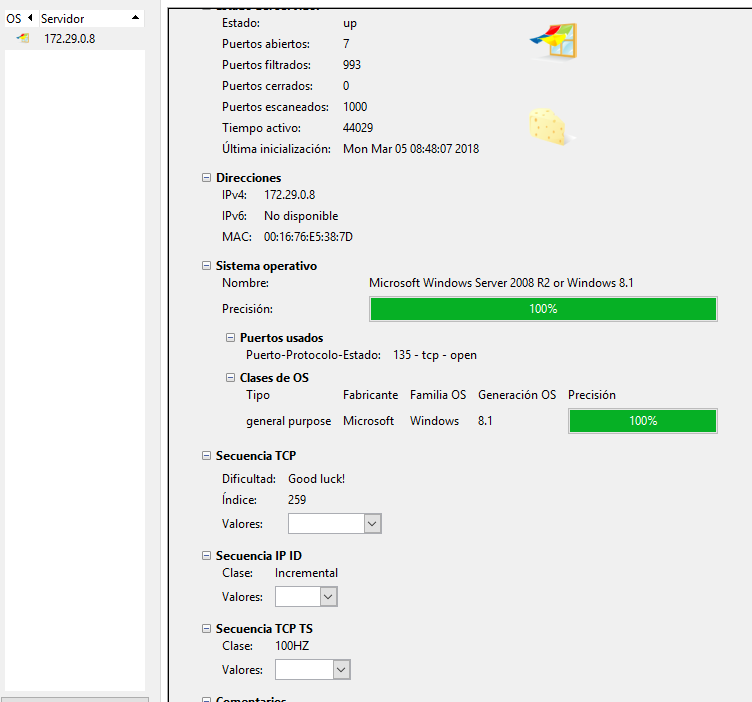
1. Ejecute un escaneo al servidor Windows que está en la Red y analice cada uno de los resultados.



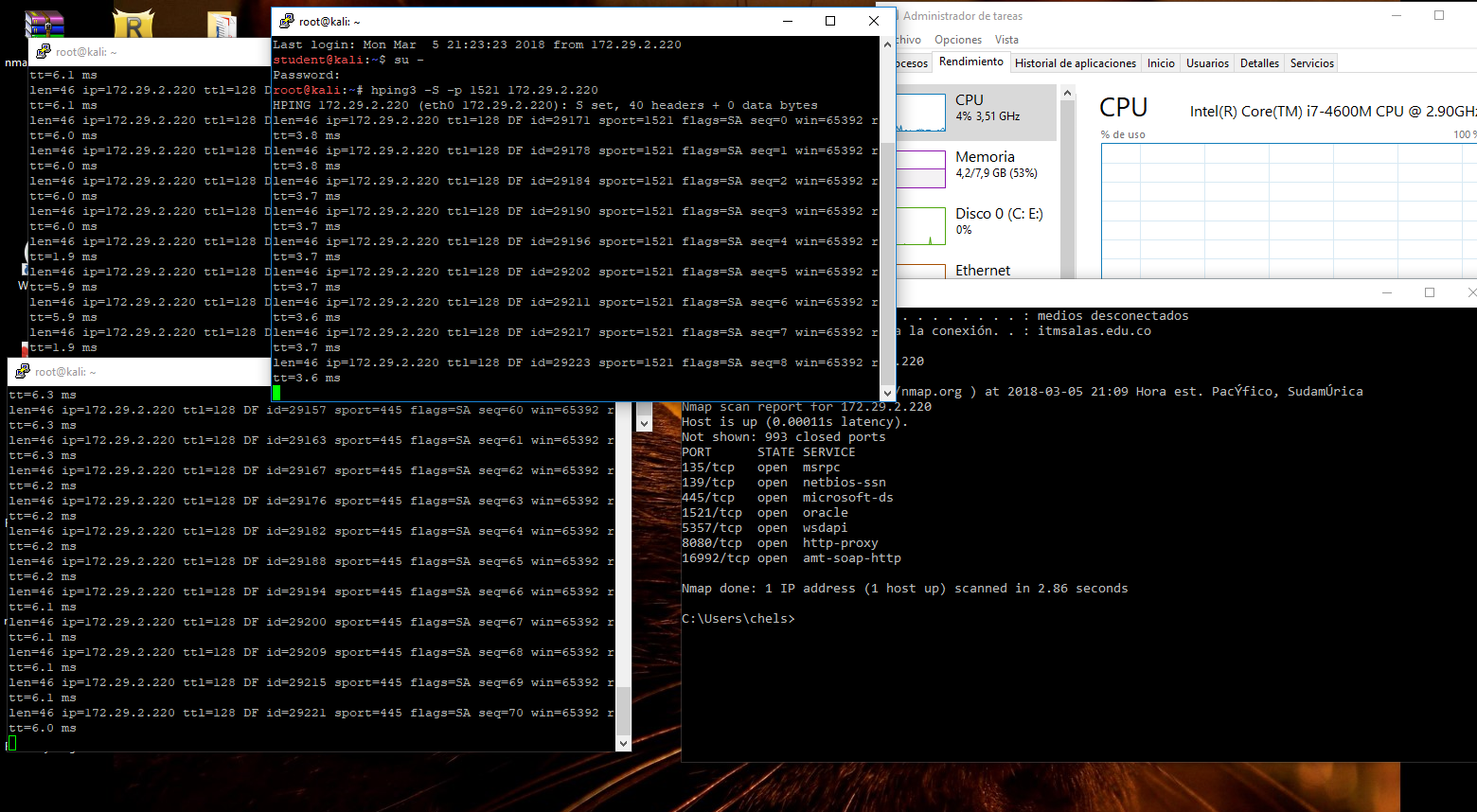
En este escaneo nos arroja







1. Ejecute un escaneo a toda la red (con máscara /24) y analice cada uno de las pestañas de nmap. Entregue una breve descripción de lo encontrado.
2. **PARTE 3 – Ataque de negación de servicio**



1. Se debe investigar, de forma breve, que hace HPING.

[HPing](http://www.hping.org/) es una herramienta en linea de comandos que nos permite crear y analizar paquetes **TCP/IP**, y como tal tiene unas muchas utilidades: hacer testing de firewalls, escaneo de puertos, redes y como no… también tiene la capacidad de provocar un**SYN Flood Attack**mediante denegación de servicio (DoS)

El objetivo de un ataque de este tipo es el envío de peticiones de conexión TCP más rápido de lo que una máquina puede procesar, al fin de saturar los recursos y evitar que la máquina pueda aceptar más conexiones.

**Para instalar la ultima versión de hping** dependiendo de la distribucion que usemos haríamos:

* En **Debian** y derivadas como **Ubuntu**y**Linux Mint**.

***sudo apt-get install hping3***

* En **Fedora**

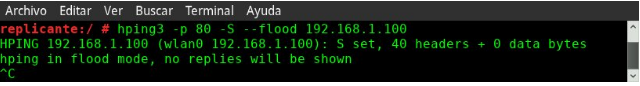
***yum install hping3***

* En **openSUSE**

***zypper install hping3***

Un ataque clásico de DDoS sería el siguiente

**hping3 -p 80  -S --flood ip\_victima**



donde:

**-p 80** es el puerto que elegimos atacar

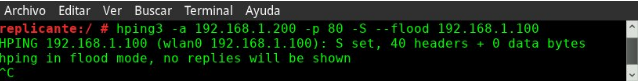
**-S** activa el flag Syn

**--flood** le indica a hping que envie los paquetes a la máxima velocidad posible

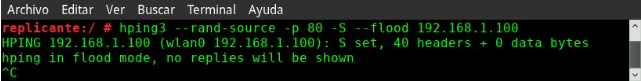
**ip\_victima** es la ip o dominio a atacar

Si queremos que nuestra**ip no sea visible** podemos añadirle la opción –a y la ip que vamos a falsear

**hping3 -a ip\_falsa -p 80  -S --flood ip\_victima**



o bien utilizar **--rand-source** con lo que se generan direcciones de origen ip al azar



Como veis en los ejemplos el testing lo he realizado sobre mi propia red…así que recordaros algo obvio, que los ataques DoS o DDoS son considerados delito en muchos países...por lo que please ser responsables con el uso que le deis.

1. Ejecute el siguiente comando:

Hping3 localhost –S –p 80 –i u1

1. Monitoreo los diferentes recursos de la maquina atacada (cpu, memoria, red) y digite lo siguiente:

hping3 <ip\_destino> -S –p <# de puerto disponible> -i u1

* 1. Que sucede con el comando anterior?
  2. Que comportamiento observa en la maquina Windows? Memoria y CPU.

**COMANDOS LINUX DE AYUDA:**

* 1. su - “comando para acceder con privilegios de root
  2. man <nombre\_de\_comando> “Manual de comandos
     1. ejemplo: man who
  3. apt-get “para instalar paquetes
  4. tail –f /var/log/messages “para ver parte de un log
  5. ls “comando para listar un directorio
  6. touch <nombre archivo> “Para crear un archivo nuevo-vacio”
  7. cd <carpeta destino> “para moverse a otro directorio.
  8. cat <nombre de archivo> “para ver el contenido de un archivo
  9. mkdir <nombre> “para crear carpetas
  10. more <nombre de archivo> “para ver el contenido de un archivo
  11. fdisk –cul “muestra la info de las particiones
  12. gedit <nombre\_archivo> “para crear archivos
  13. cp <origen> <destino> “copiar archivos
  14. mv <origen> <destino> “mover archivos
  15. rm <nombre\_archivo> “para remover un archivo
  16. rmdir <nombre\_archivo> “para remover una carpeta
  17. top “ver el uso de CPU y procesos.
  18. service <nombre\_del\_servicio> status “verifica el estado de un servicio,
      1. ejemplo: service httpd status
      2. ejemplo: service httpd start

Otros comandos:

1. ps aux - ver procesos en ejecución
2. free - ver espacio en disco
3. df –h - particiones de discos duros
4. pwd - en que carpeta estoy ejecutando
5. dpkg –l - lista de paquetes de softwware
6. hostname - nombre del equipo
7. ifconfig –a - configuración de la tarjeta de red
8. clear - limpiar pantalla
9. para listar directorio:
   * 1. ls -l
     2. ls –al
     3. ls –alt
10. **Incluir usuarios a grupos y permisos sobre grupos y archivos.**

**chmod** Cambia los permisos de los archivos.

**groupadd** Añade un nuevo grupo al sistema

**useradd** Añade un nuevo usuario al sistema

-g

-d

-m

-s

**userdel** borrar un usuarios

**chown** Permite cambiar a los dueños de  los archivos

**passwd** cambio de contraseña a los usuarios.