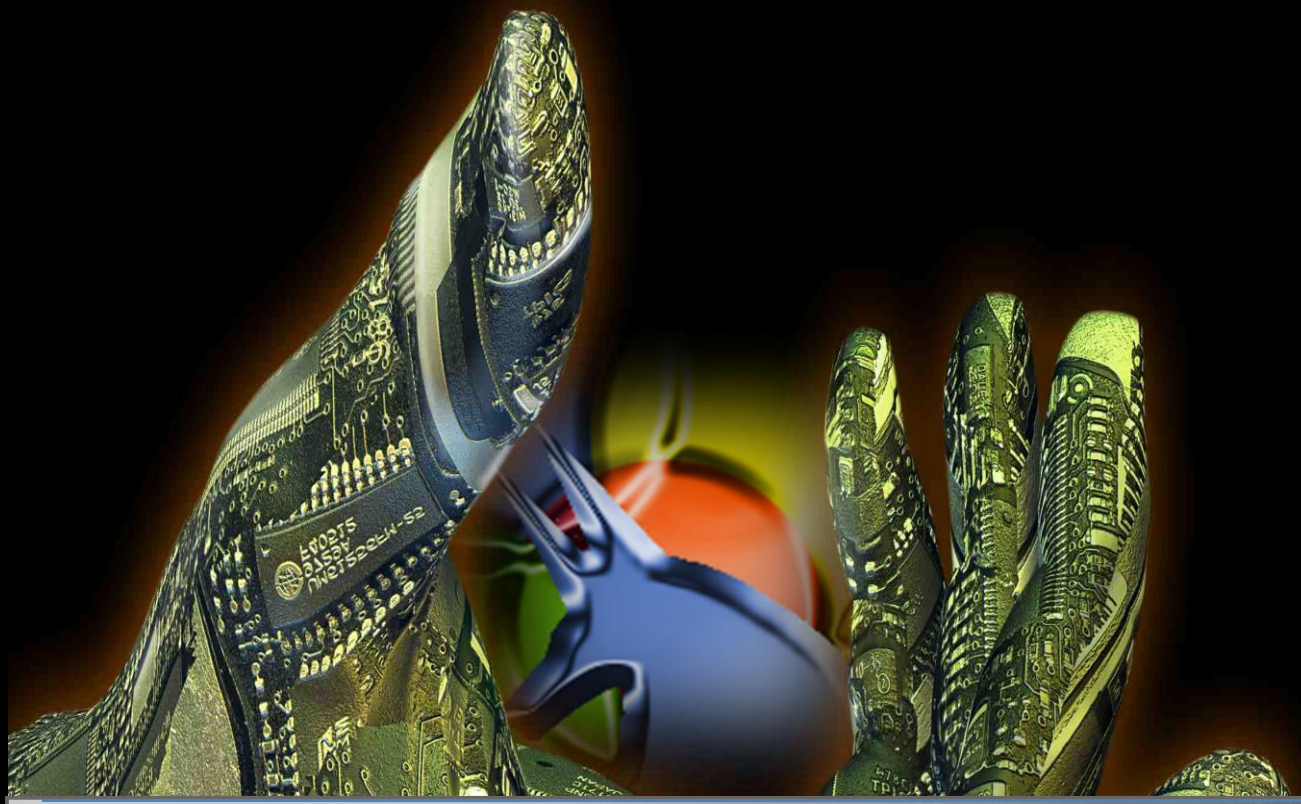
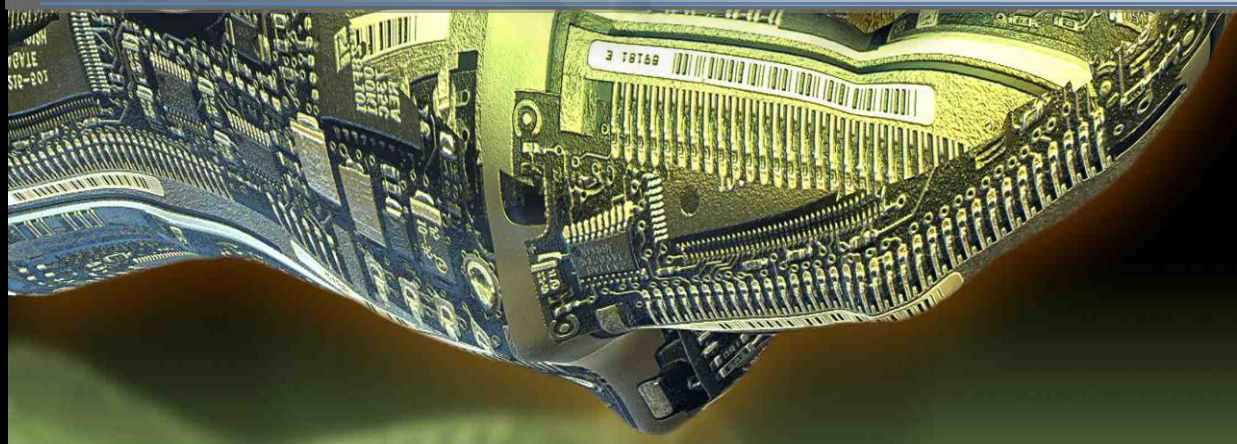
4/4/2010



ANUBIS: Manual de Usuario



Herramienta para la automatización de los Procesos de Footprinting y Fingerprinting durante las Auditorías de Seguridad Informática

Juan Antonio Calles García

Índice

Este manual pretende explicar el funcionamiento básico de la herramienta Anubis, diseñada para facilitar los procesos de Footprinting y Fingerprinting durante las Auditorías de Seguridad Informática.

Anubis incorpora dos tipos de herramientas, las herramientas lanzadera y las herramientas de realimentación. Las primeras se encargan de obtener toda la información pública o publicada descuidadamente de una organización, almacenarla y presentarla de una manera lógica y visible. Las herramientas lanzadera que incorpora Anubis son:

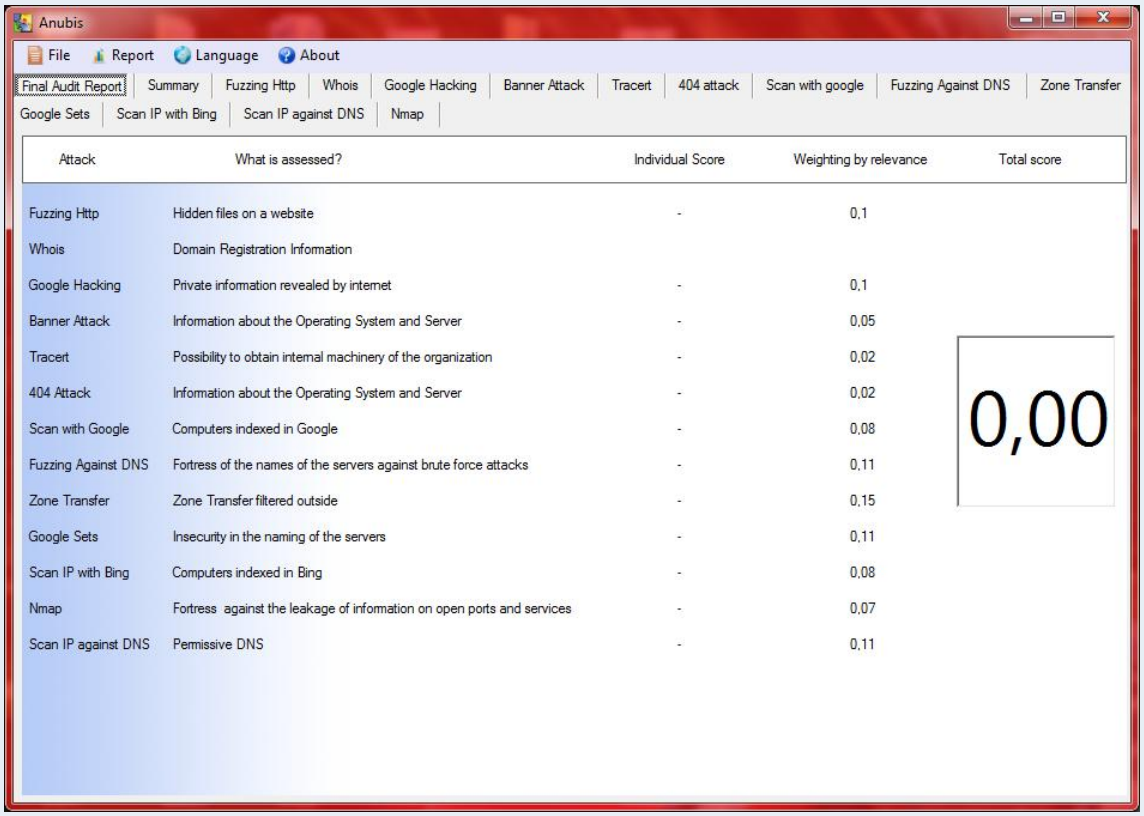
1. Fuzzing Http
2. Whois
3. Google Hacking
4. Banner Attack
5. 404 Attack
6. Scan with Google
7. Fuzzing against DNS
8. Zone Transfer

El segundo tipo de herramientas pretenden buscar más información a partir de la ya encontrada, aumentando la información obtenida en gran medida. Estas herramientas tienen mayor potencial que las anteriores pero dependen del éxito de las herramientas lanzadera para operar:

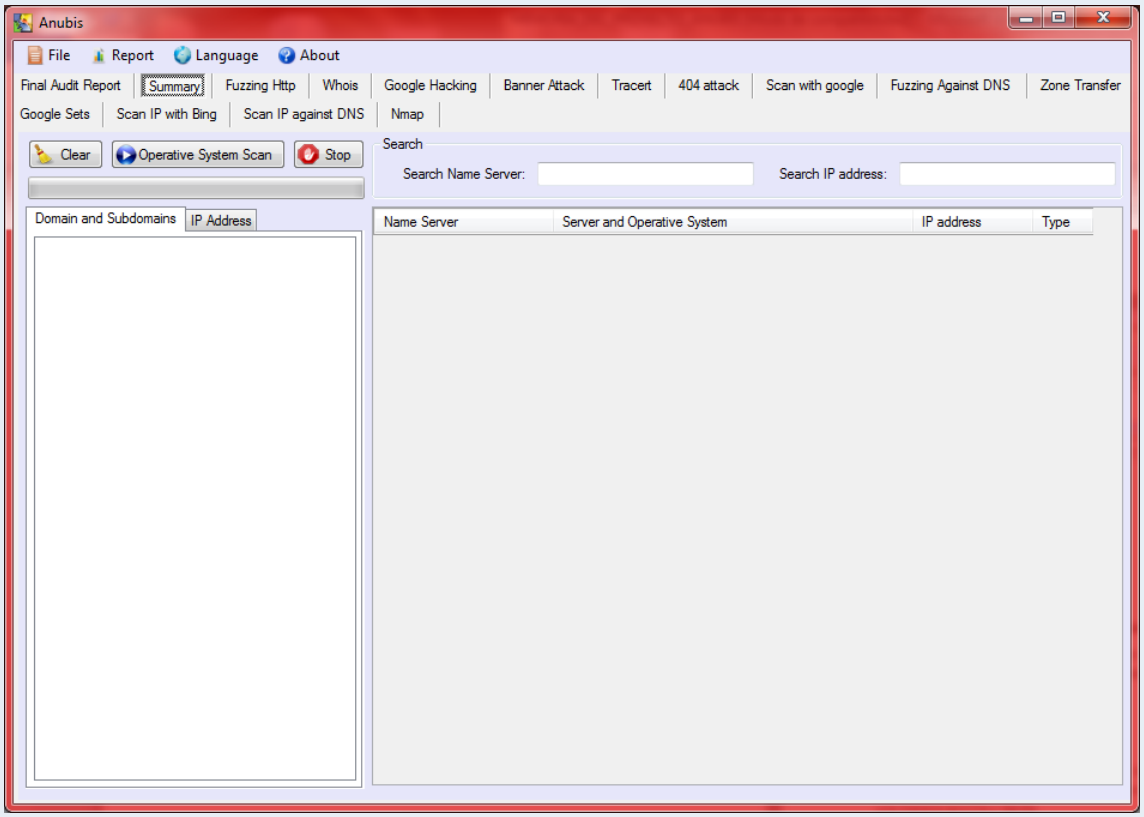
1. Google Sets
2. Scan IP with Bing
3. Fuzzing against DNS
4. Scan IP against DNS
5. NMap

Una vez finalizados los escaneos con las distintas herramientas, Anubis presenta un informe del estado de la organización, y permite exportarlo de diferentes formas a HTML y a XML para poder transportarlo, presentarlo en el informe final de una auditoría o utilizarlo en otras herramientas que interpreten XML o cargar el proyecto posteriormente en Anubis para poder utilizar los datos tras cerrar el programa.

Al abrir el programa se puede ver la pantalla inicial donde Anubis mostrará al finalizar la auditoría un resumen del estado de la organización:



Inmediatamente después, en la segunda pestaña se encuentra el resumen de las máquinas y dominios encontrados durante la auditoría presentados en forma de tabla y de árbol jerárquico.



A partir de la tercera pestaña se encuentran todas las herramientas nombradas al principio de este punto con las que se realizarán las labores pertinentes de auditoría.

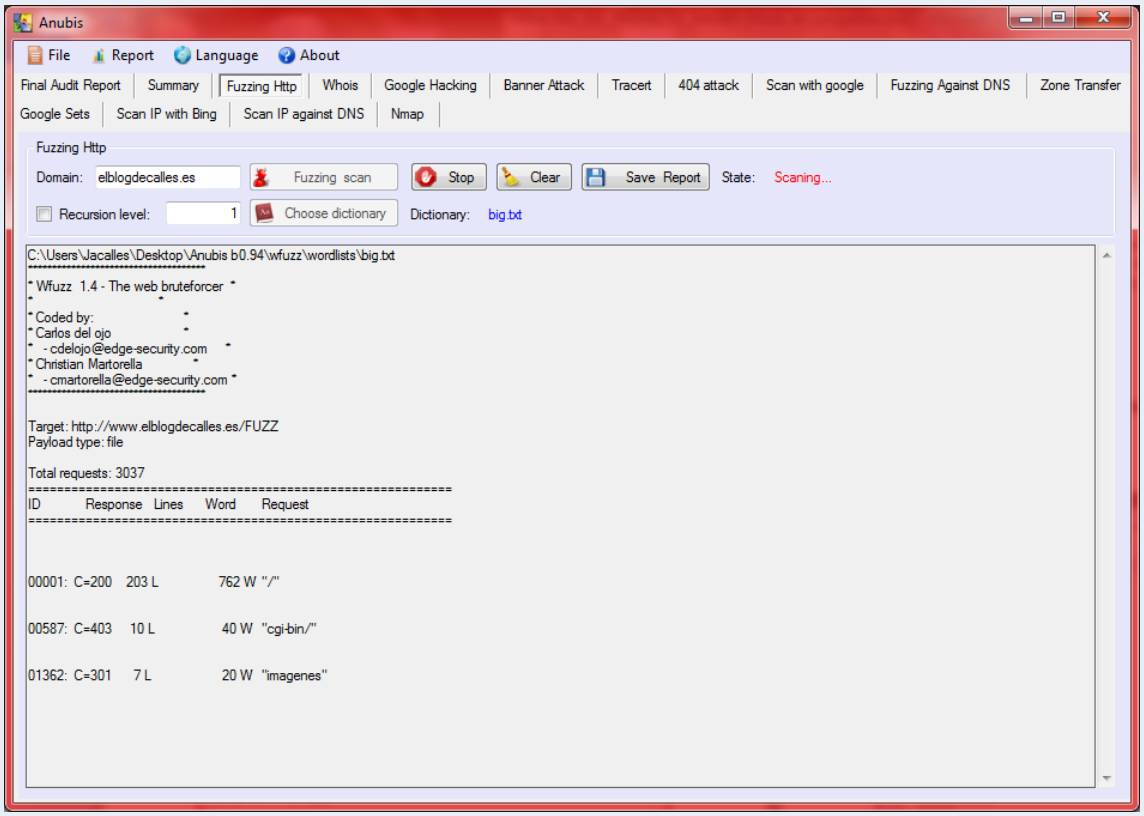
HERRAMIENTAS LANZADERA

Fuzzing HTTP

La herramienta *Fuzzing HTTP* automatiza el lanzamiento del programa WFUZZ, de "*Edge-Security",* que permitirá localizar ficheros y zonas ocultas en un sitio web, de una manera sencilla y rápida.

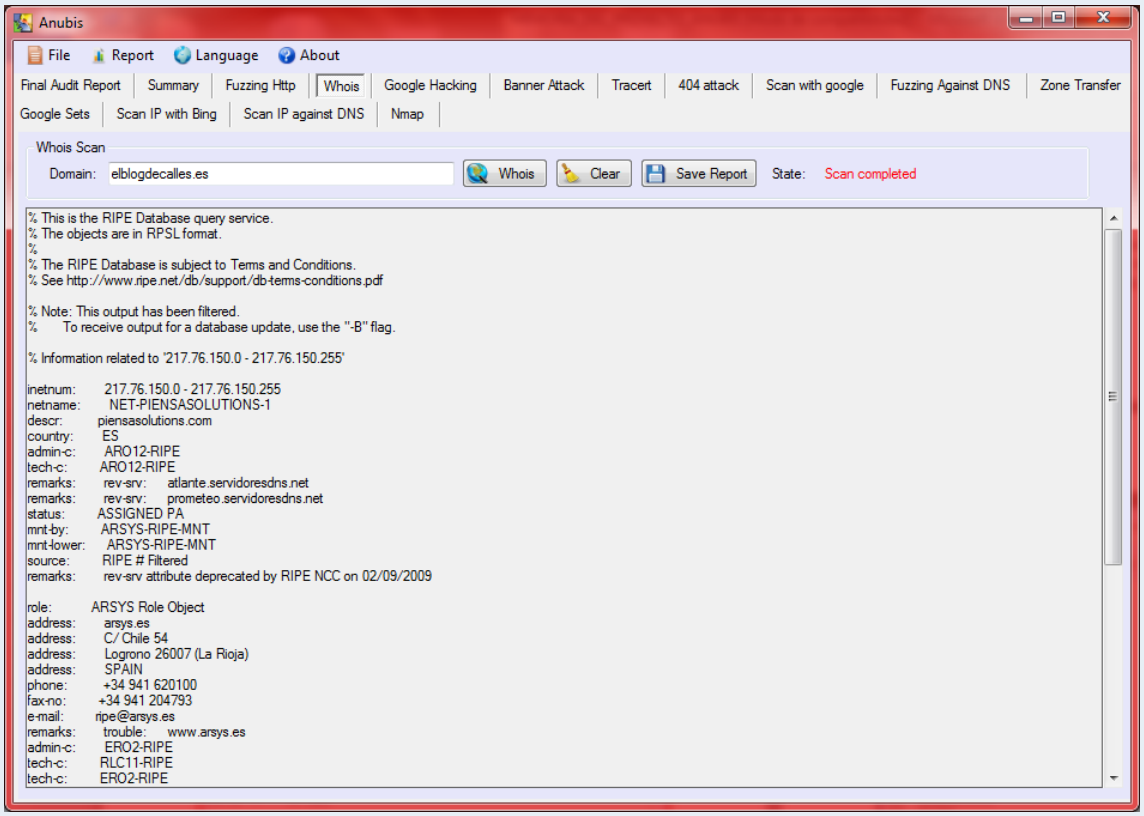
Para lanzar *Fuzzing HTTP* en primer lugar hay que seleccionar un diccionario (por defecto seleccionado el diccionario big.txt). Los diccionarios se encuentran en la ruta "*wfuzz**wordlists*", dentro de la raíz del proyecto. Después habrá que elegir el nivel de recursividad del ataque, es decir, si encuentra una carpeta, el número de subcarpetas que se desea reciban otro escaneo completo. Y finalmente se selecciona el botón *Fuzzing Scan*.

Para detener el escaneo basta con pulsar en cualquier momento el botón Stop. Si se desea guardar la información obtenida, se seleccionará la opción guardar, que permitirá almacenar el reporte en formato txt:



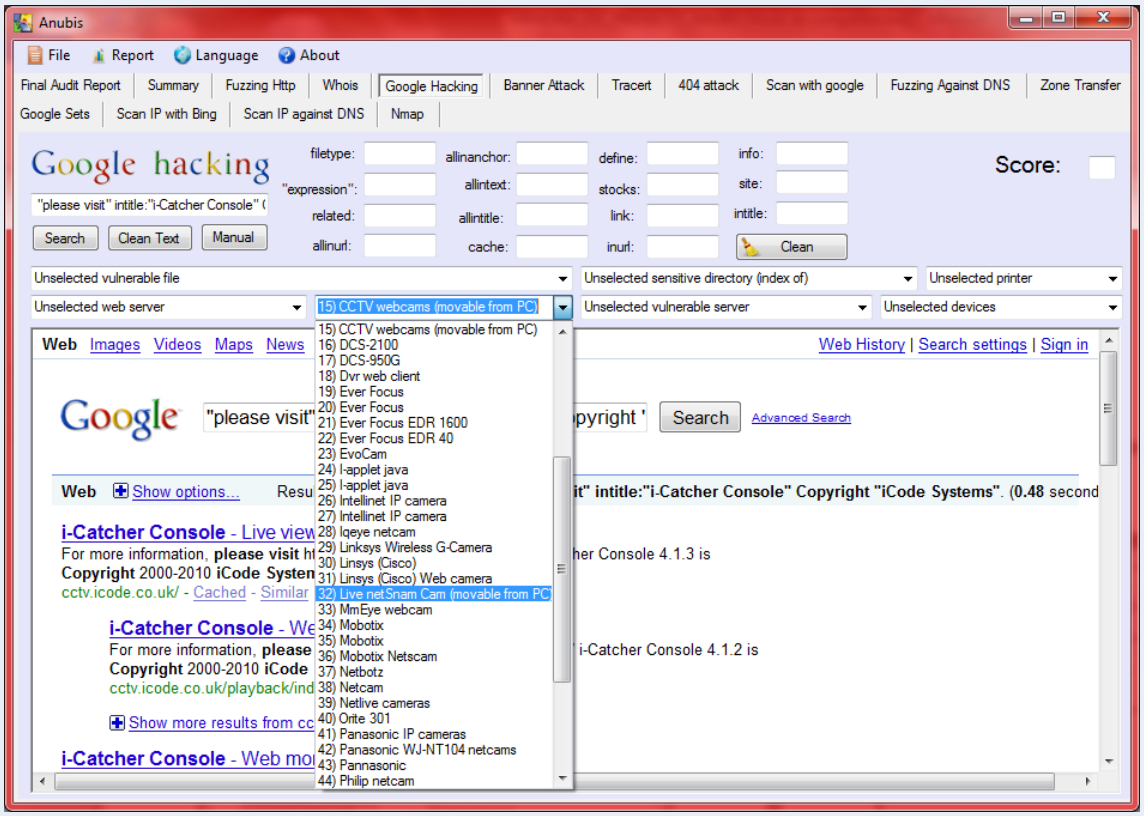
WHOIS

La herramienta Whois permitirá ver la información del usuario que ha registrado un dominio. Su uso es sencillo, en primer lugar se introducirá un dominio y después se pulsará el botón “Whois”. Al igual que en la anterior herramienta, es posible guardar un reporte en .txt.



Google Hacking

La herramienta Google Hacking lleva incorporado un navegador web desde el que se podrán lanzar “queries” típicas de Google Hacking desde cualquiera de sus casillas. Además lleva incorporados escaneos predefinidos, como por ejemplo el escaneo de cámaras web que se puede ver en la siguiente imagen:



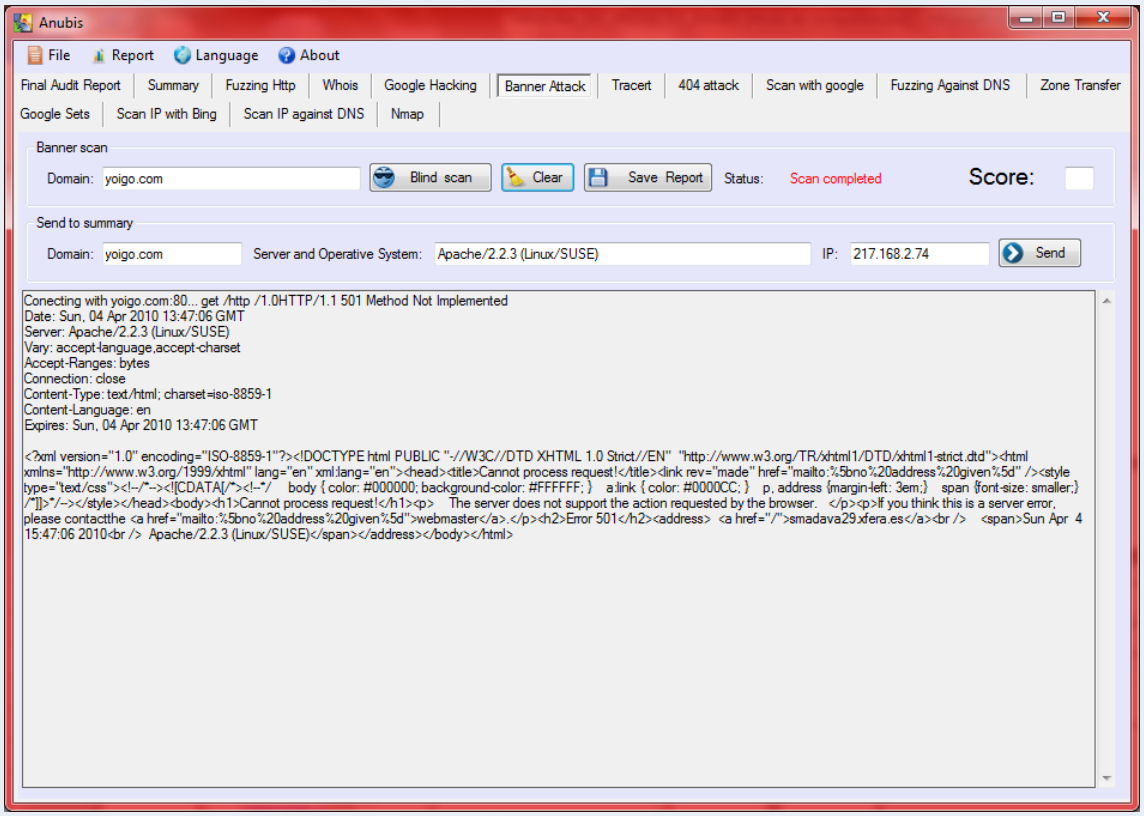
Una vez finalizada la parte de la auditoría dedicada a la búsqueda de información con Google se deberá valorar con una nota de 0 a 10 el estado de la organización. Las notas que asigne el auditor o Anubis (en las herramientas que asigna una nota automáticamente) influirán en la nota final que obtenga la organización y que aparecerá en el informe final.

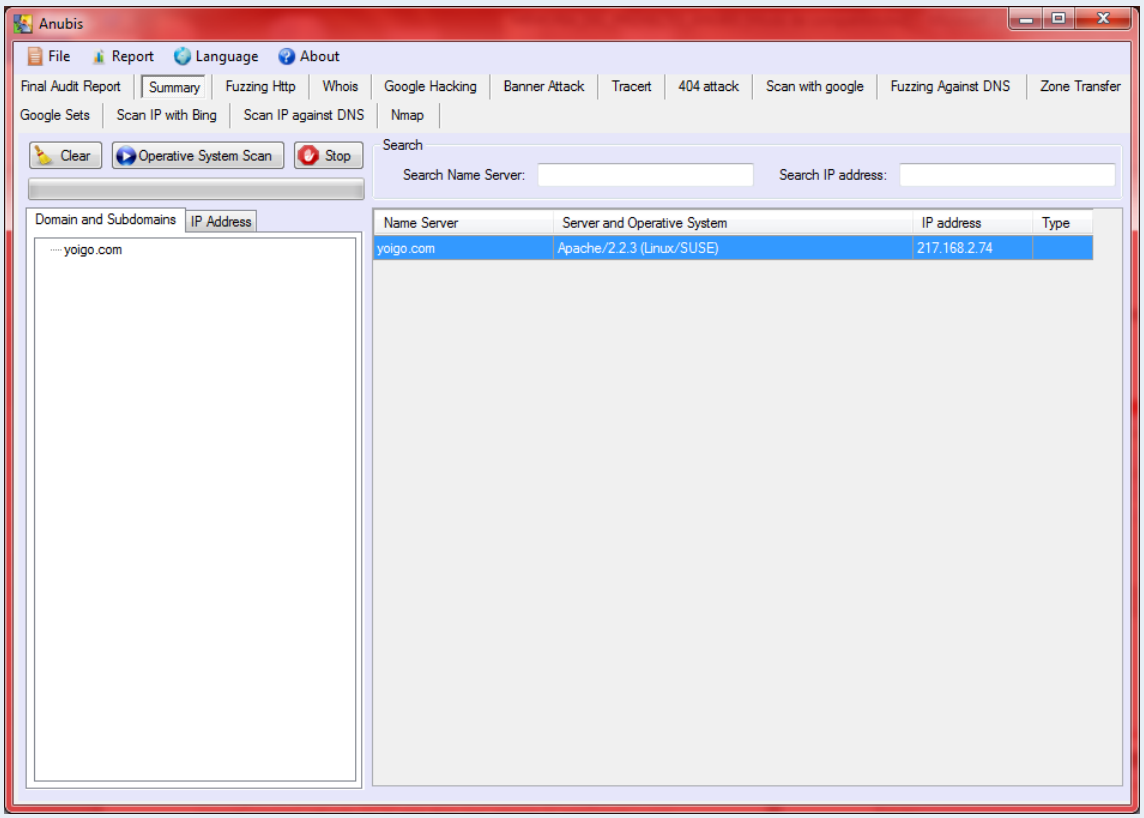
Banner Attack

Esta herramienta permite visualizar el banner del servidor web para intentar detectar el tipo de servidor y el sistema operativo utilizado en la organización. Para utilizarlo simplemente hay que indicarle un dominio y pulsar el botón de escaneo.

Al igual que en las anteriores herramientas es posible guardar el reporte en un txt. Por otro lado al igual que en Google Hacking se debe valorar de 0 a 10 el estado del banner dependiendo de si la información proporcionada se cree que es correcta o por el contrario se tiene la creencia de que ha sido modificada para engañar a los "*hackers*".

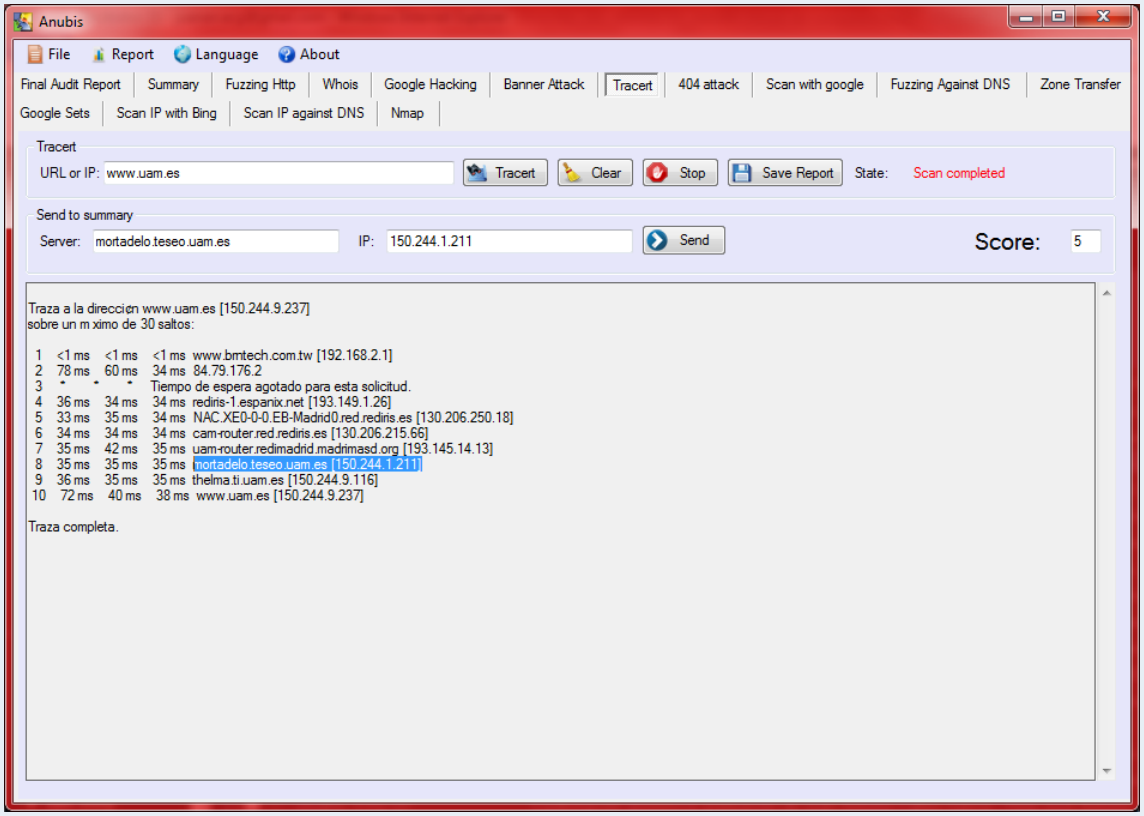
Tras realizar el escaneo se pulsará el botón *Send*. Con ello se comienza a almacenar en la tabla y en el árbol de *Summary* las primeras máquinas y dominios de la organización:


Anubis
File
Report
Language
About
Final Audit Report
Summary
Fuzzing Http
Whois
Google Hacking
Banner Attack
Tracert
404 attack
Scan with google
Fuzzing Against DNS
Zone Transfer
Google Sets
Scan IP with Bing
Scan IP against DNS
Nmap
Banner scan
Domain: yoigo.com
Blind scan
Clear
Save Report
Status: Scan completed
Score:
Send to summary
Domain: yoigo.com
Server and Operative System: Apache/2.2.3 (Linux/SUSE)
IP: 217.168.2.74
Send
Conecting with yoigo.com:80... get /http /1.0HTTP/1.1 501 Method Not Implemented
Date: Sun, 04 Apr 2010 13:47:06 GMT
Server: Apache/2.2.3 (Linux/SUSE)
Vary: accept-language,accept-charset
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=iso-8859-1
Content-Language: en
Expires: Sun, 04 Apr 2010 13:47:06 GMT
<?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en"><head><title>Cannot process request!</title><link rev="made" href="mailto:%5bno%20address%20given%5d" /><style type="text/css"><!--/*--><![CDATA[/*><!--*/ body { color: #000000; background-color: #FFFFFF; } a:link { color: #0000CC; } p, address {margin-left: 3em;} span {font-size: smaller;} /*]]>*/--></style></head><body><h1>Cannot process request!</h1> The server does not support the action requested by the browser. If you think this is a server error, please contactthe webmaster. <h2>Error 501</h2><address> smadava29.xfera.es
 Sun Apr 4 15:47:06 2010
 Apache/2.2.3 (Linux/SUSE)</address></body></html>


Anubis
File
Report
Language
About
Final Audit Report
Summary
Fuzzing Http
Whois
Google Hacking
Banner Attack
Tracert
404 attack
Scan with google
Fuzzing Against DNS
Zone Transfer
Google Sets
Scan IP with Bing
Scan IP against DNS
Nmap
Clear
Operative System Scan
Stop
Search
Search Name Server:
Search IP address:
Domain and Subdomains
IP Address
yoigo.com
Name Server
Server and Operative System
IP address
Type
yoigo.com
Apache/2.2.3 (Linux/SUSE)
217.168.2.74

TRACERT

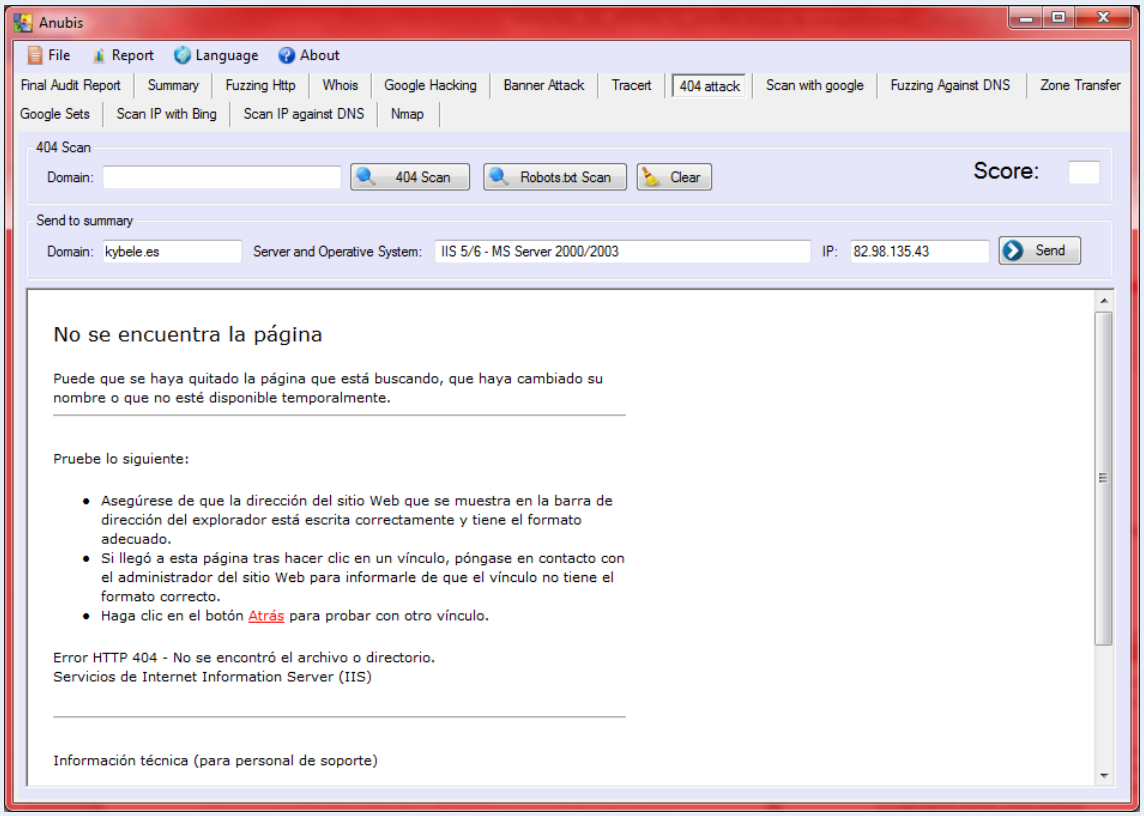
La herramienta *Tracert* permite hacer una traza de los puntos por donde pasa una petición web hasta resolverse. Para utilizarla basta con añadir una URL o una dirección IP y pulsar el botón *Tracert*.



Tras hacer una traza en numerosas ocasiones se puede ver como aparece algún servidor de la organización por el que pasa, como se puede ver en la imagen anterior. Estos servidores al igual que en el *Banner Attack* podrán ser agregados a la tabla de máquinas de la organización que hay en *Summary*, para ello bastará con añadir la máquina y la IP en las casillas habilitadas para ello y pulsar el botón *Send*. Finalmente se debe valorar el escaneo con una nota de 0 a 10.

404 Attack

Esta herramienta permite lanzar una URL malformada para intentar provocar el error 404 en el navegador, con lo que se conseguirá, de tener el Servidor Web con la configuración por defecto, mostrar el modelo de Servidor. Su funcionamiento es sencillo, en primer lugar se inserta un dominio y finalmente se pulsa el botón *Scan*:



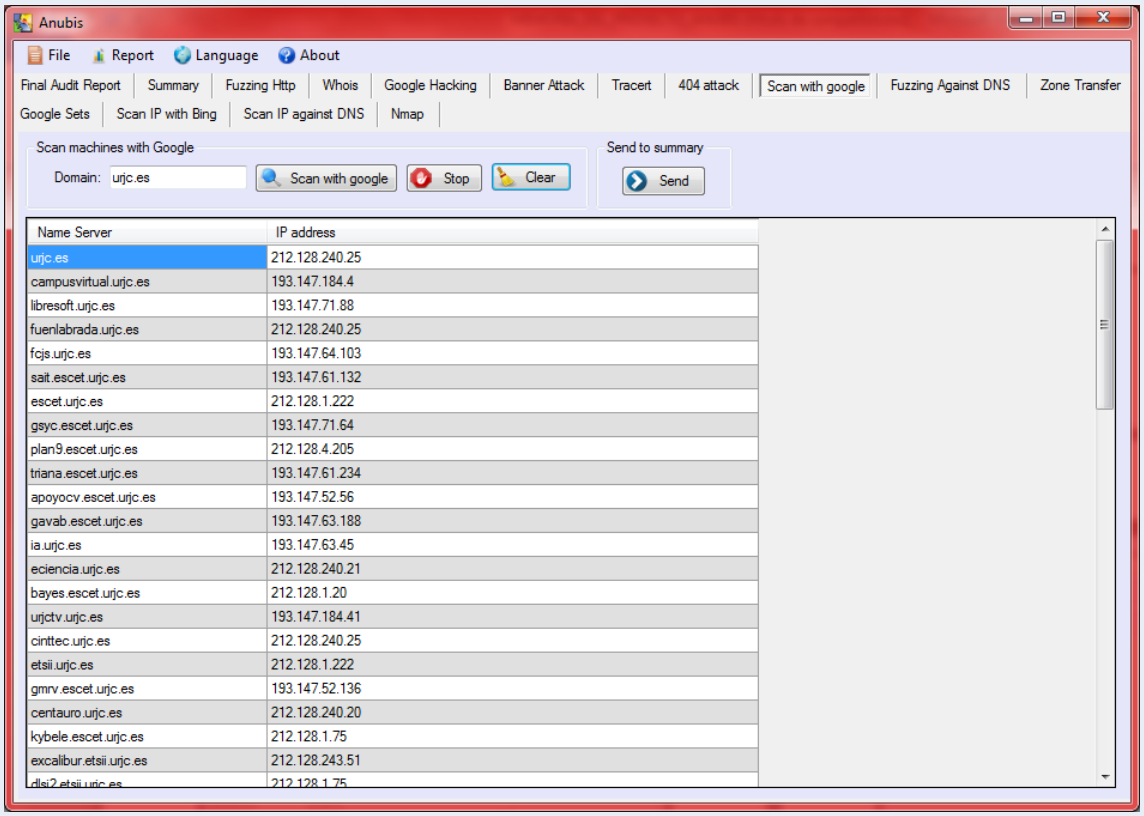
Una vez finalizado el escaneo si ha habido éxito se indicará un posible tipo de servidor y sistema operativo y permitirá añadirlo a la tabla de máquinas de la organización pulsando el botón *Send*.

Además se podrá visualizar el archivo *robots.txt* (en caso de que existiese) y en el que se puede encontrar en ocasiones rutas ocultas en una web, al igual que con la herramienta *Fuzzing Http*. Finalmente se valorará con una nota de 0 a 10 el estado de la organización frente a este escaneo.

Scan with google

Éste escaneo permite mediante búsquedas hacking en Google encontrar todos los dominios, subdominios y máquinas que hay indexadas en Google. Con esta herramienta se conseguirá información muy valiosa para añadir a la tabla de máquinas y al árbol de la red de la organización que hay en la pestaña *Summary*. Ésta herramienta es de vital importancia para el lanzamiento posterior de las herramientas de realimentación.

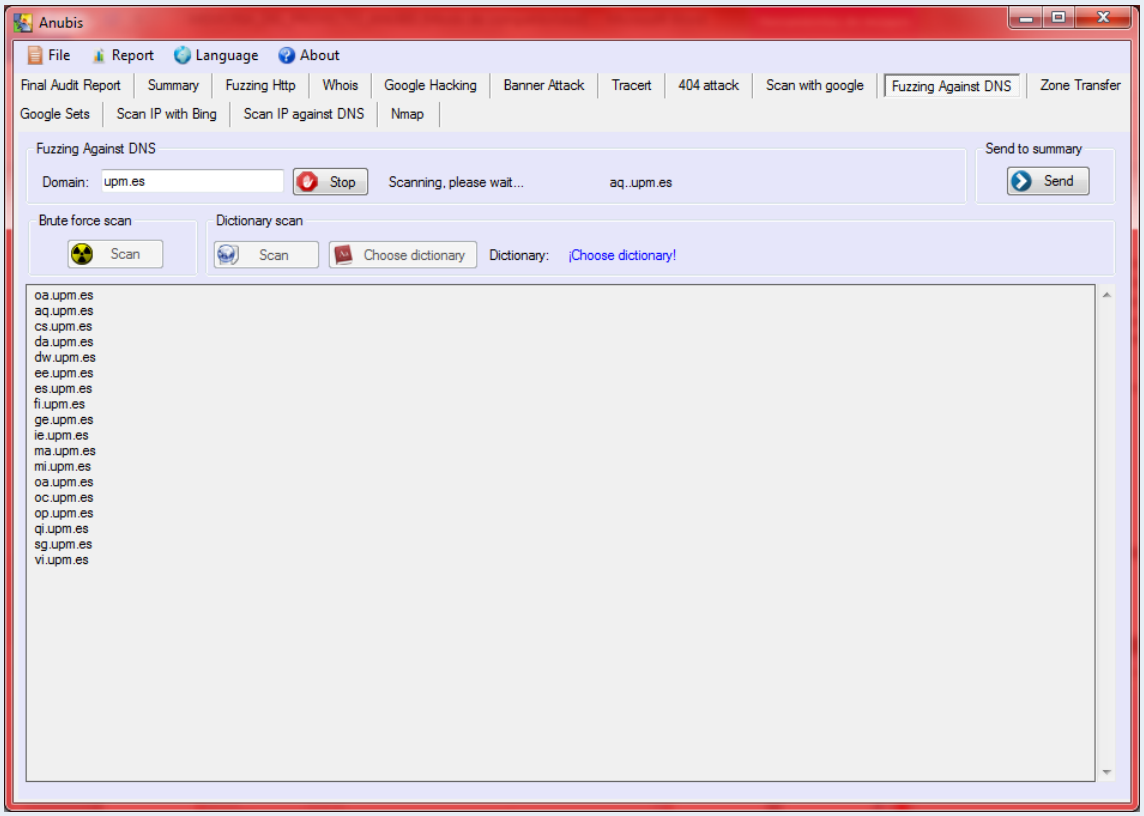
En grandes organizaciones será normal ver cómo encuentra más de 500 subdominios:



Para lanzar el escaneo se debe insertar un dominio y pulsar el botón *Scan*. Finalmente se podrán añadir todas las máquinas a la tabla y al árbol que simulará el mapa de la organización de la pestaña *Summary* pulsando *Send*. En esta ocasión Anubis será el encargado de poner una nota de 0 a 10 al estado de la organización dependiendo del número de información obtenida.

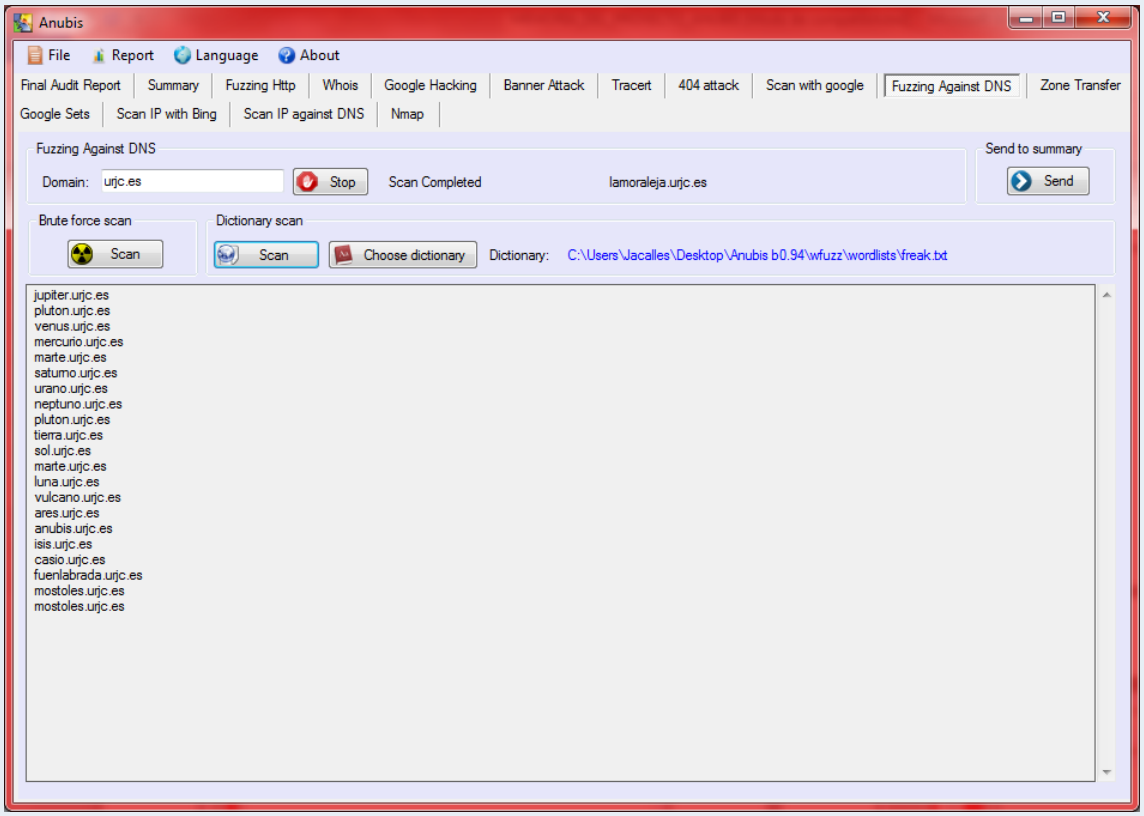
Fuzzing against DNS

Esta herramienta permitirá hacer dos tipos de ataques contra el DNS para intentar obtener el mayor número de máquinas internas de la organización. El primero de los ataques consistirá en lanzar un ataque de fuerza bruta mediante permutaciones infinitas de símbolos y caracteres alfanuméricos, que deberá pararse manualmente cuando se crea pertinente. Para utilizarlo se debe introducir un dominio y pulsar el botón *Scan* que aparece con el símbolo nuclear:



Ésta herramienta es lenta ya que las permutaciones van aumentando de manera exponencial, pero es muy eficaz.

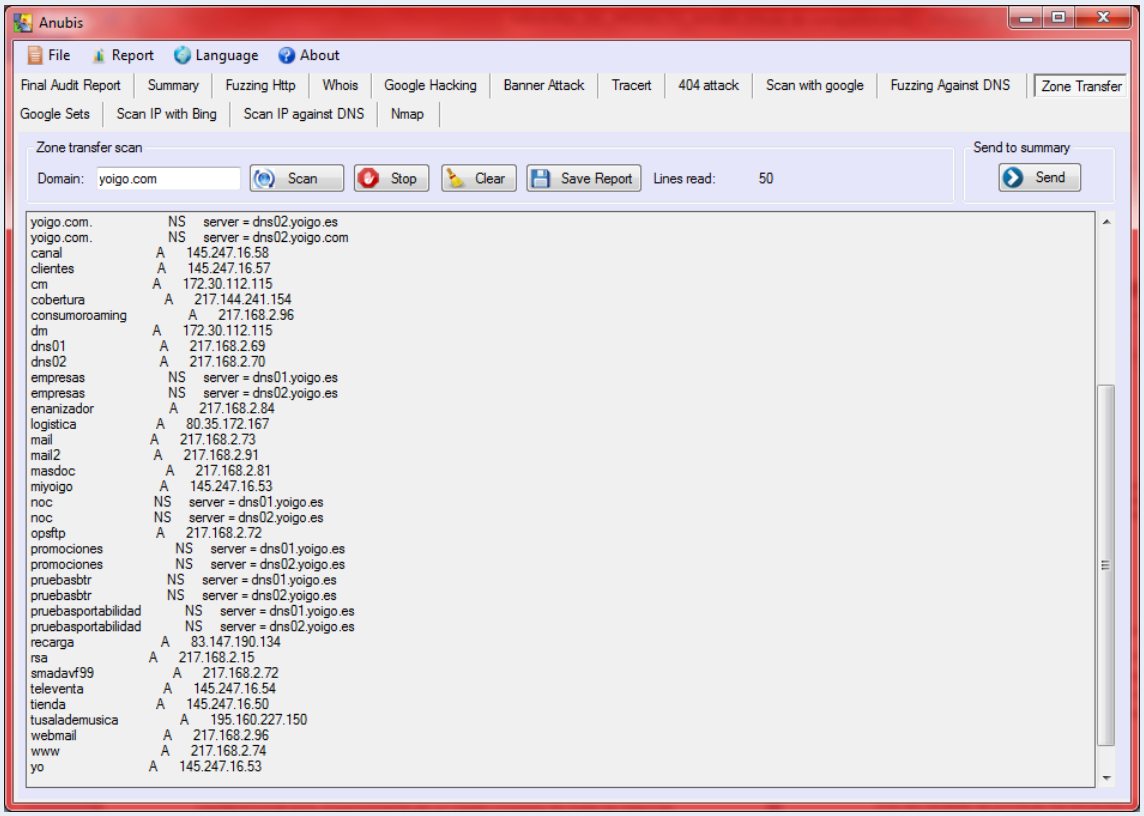
La segunda herramienta permitirá barrer el DNS con un ataque por diccionario, bien aprovechando los diccionarios de WFUZZ, bien añadiendo nuevos diccionarios manualmente, o bien utilizando un diccionario que se ha diseñado especialmente para atacar servidores, que contiene nombres “freaks” que los administradores suelen dar a sus servidores. Este diccionario se le ha denominado freak.txt y se puede encontrar en la misma carpeta que los diccionarios de WFUZZ. Para lanzar el escaneo, tras seleccionar un diccionario, basta con pulsar el botón Scan que tiene el icono de de la tierra:



Finalmente se podrán añadir todas las máquinas a la tabla y al árbol que simulará el mapa de la organización de la pestaña *Summary* pulsando *Send*. En esta ocasión Anubis será el encargado de poner una nota de 0 a 10 al estado de la organización dependiendo del número de información obtenida.

Zone Transfer

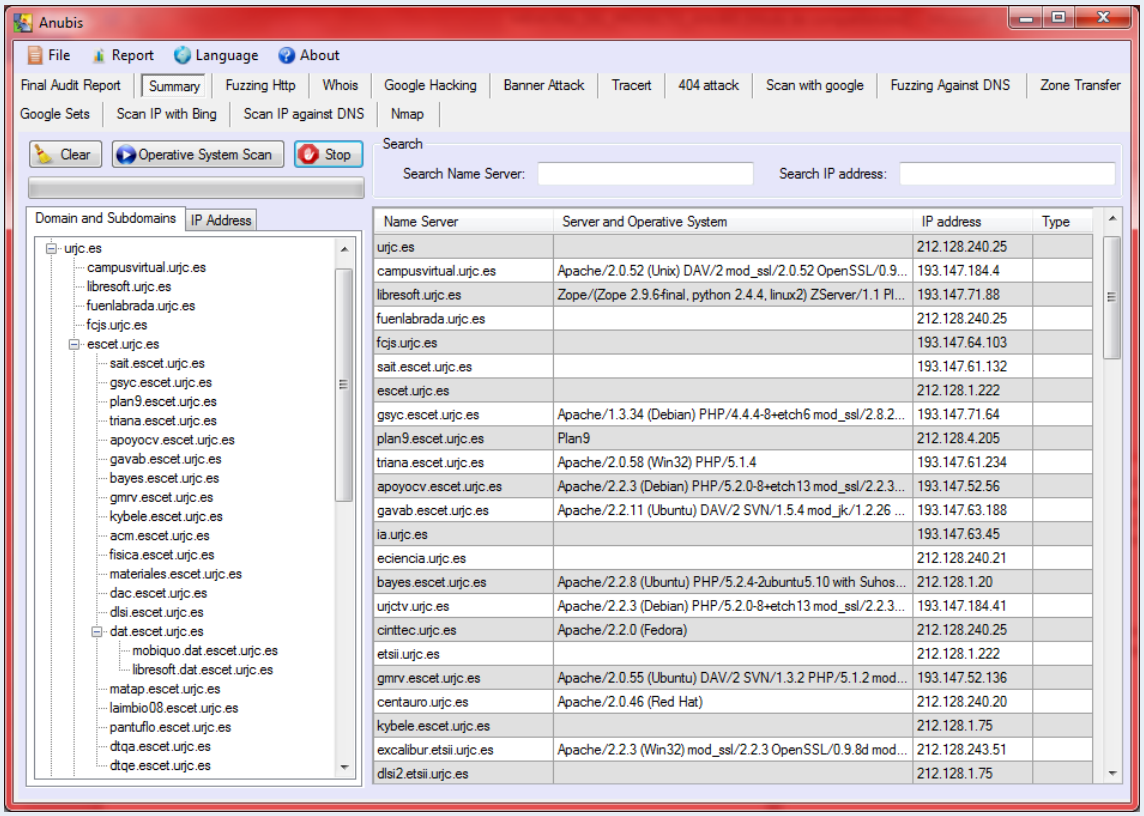
Esta herramienta comprobará si alguno de los servidores de DNS padece una transferencia de zona, proporcionando así un listado completo de todas las máquinas de la organización, y casi finalizando en éste punto la parte de la auditoría dedicada a búsqueda de información. Aunque cada vez menos organizaciones padecen este error, aún son muchas las que son susceptibles a este descuido. Para lanzar el escaneo basta con introducir un dominio y seleccionar el botón *Scan*:



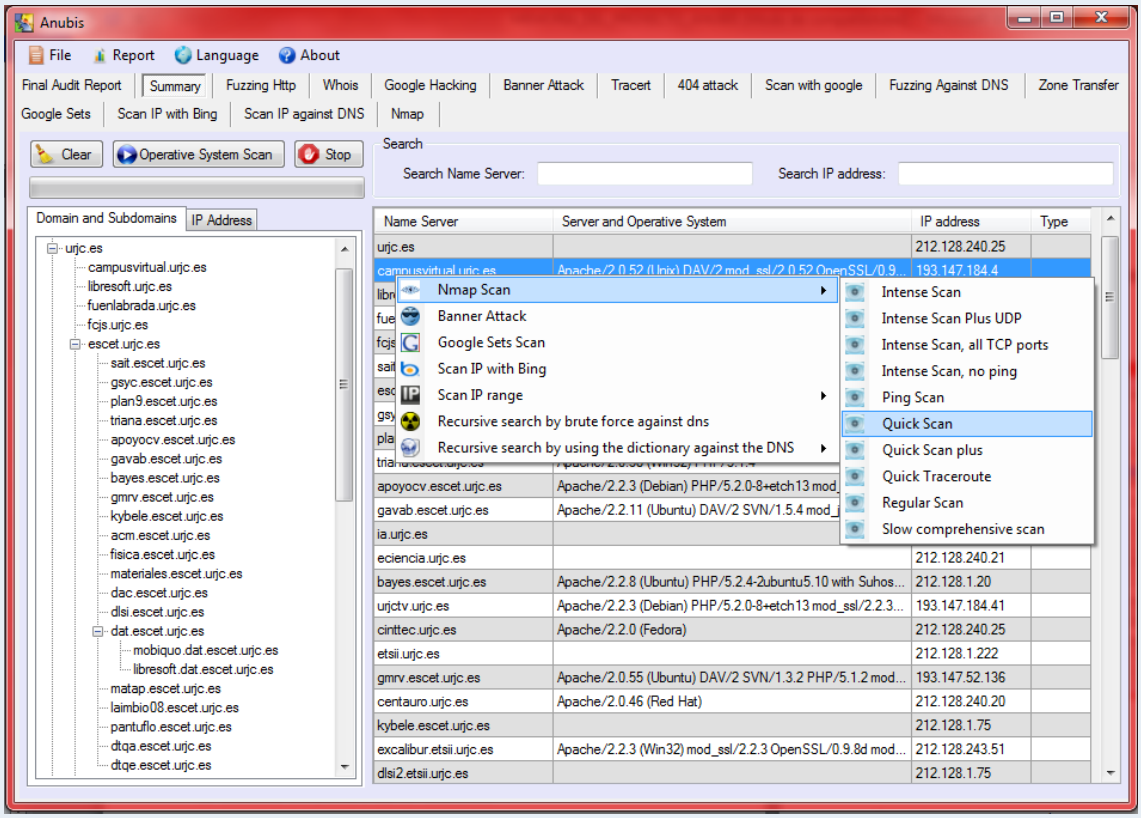
Finalmente se podrán añadir todas las máquinas a la tabla y al árbol que simulará el mapa de la organización de la pestaña *Summary* pulsando *Send*. En esta ocasión Anubis será el encargado de poner una nota de 0 a 10 al estado de la organización dependiendo del número de información obtenida.

Summary

Una vez lanzadas las primeras herramientas de búsqueda, si se accede a la pestaña *Summary,* se puede ver un gran número de máquinas internas e IP's, y un mapa de la red en forma de árbol.



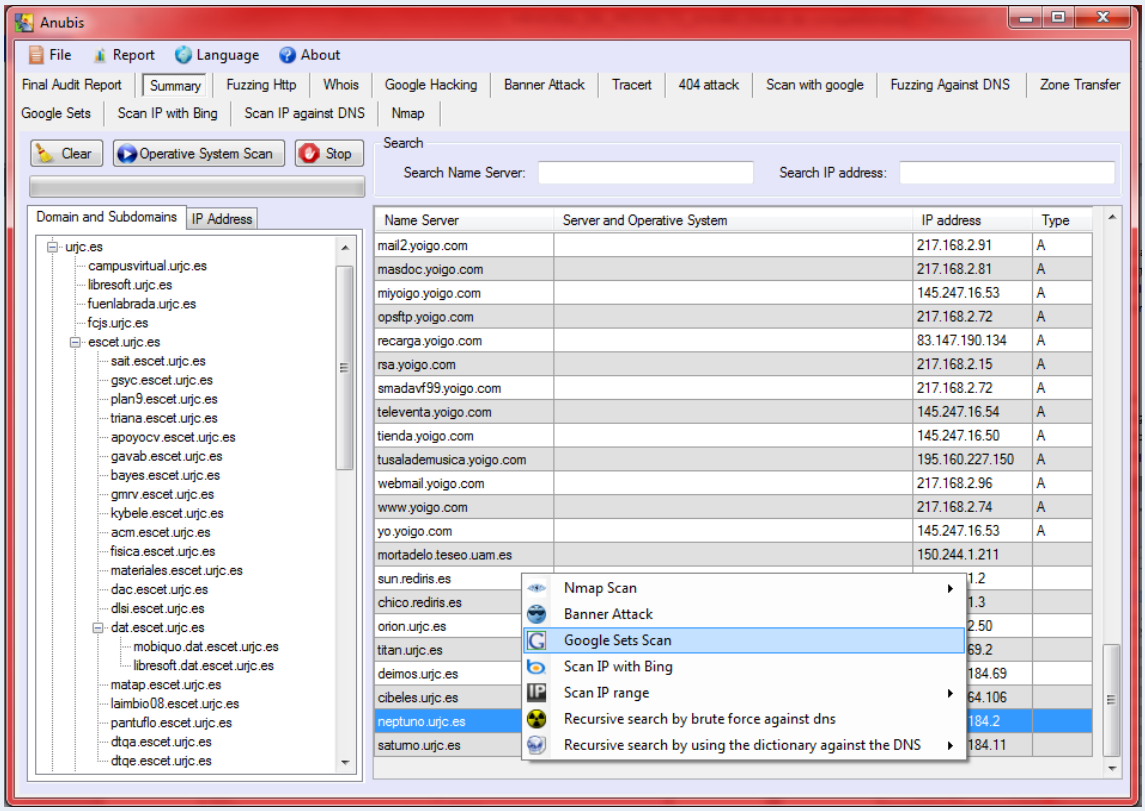
Si aún queda información por obtener se podrán utilizar las herramientas de realimentación, que se lanzan de manera automática seleccionando en la tabla de la opción *Summary* una máquina (una fila) con el botón izquierdo del ratón y pulsando botón derecho sobre ella. Se desplegará un abanico de ataques disponibles, y bastará con seleccionar uno para continuar con los escaneos:



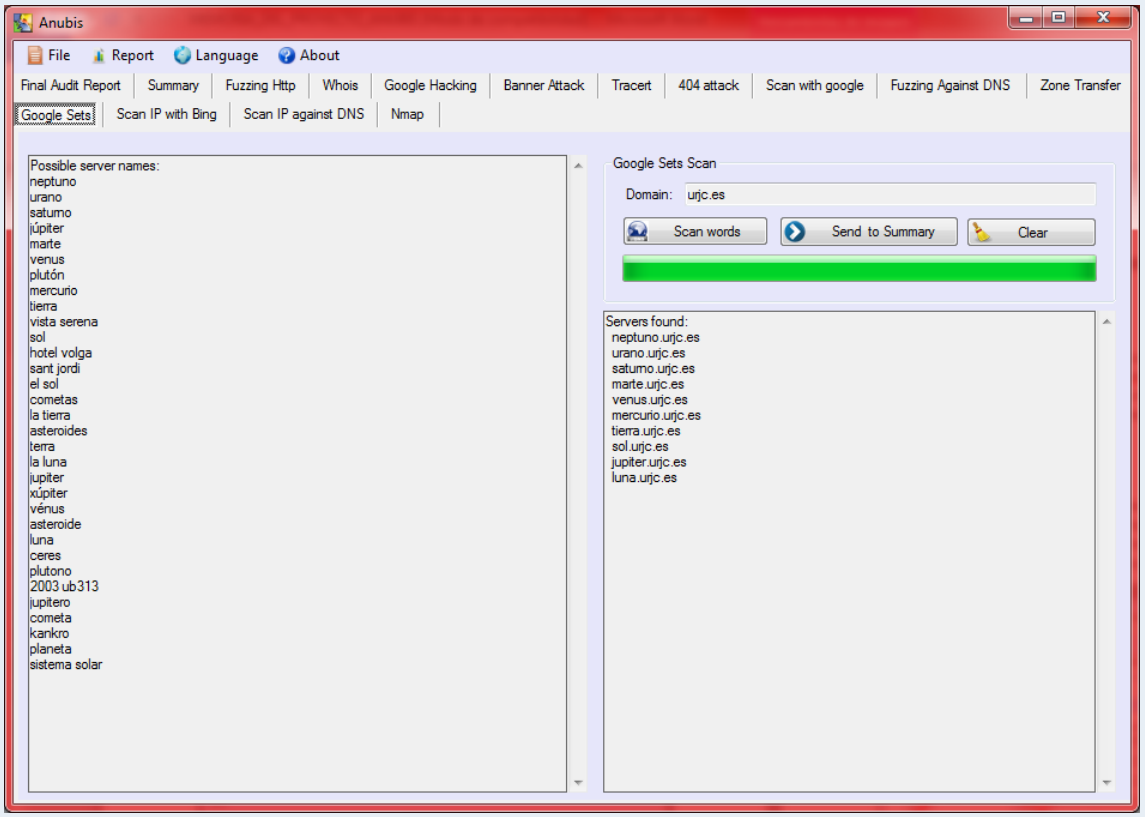
Herramientas de Realimentación

Google Sets

Google Set junto con las demás herramientas de realimentación se lanza desde el menú de opciones que se abre pulsando el botón derecho del ratón sobre la tabla *Summary*. Para arrancar el escaneo de *Google Set* bastará con seleccionar previamente una máquina de la tabla *Summary*, y desde el menú del botón derecho del ratón seleccionar Google Sets. Con este escaneo Anubis buscará palabras relacionadas con el nombre de esa máquina para intentar obtener más máquinas que el administrador haya nombrado con nombres semejantes. Por ejemplo, si un administrador llama a una máquina *litio*, es probable que exista una máquina *sodio*, o una máquina *benceno*. Todo ello lo hace gracias a la herramienta Google Set que ha diseñado Google:



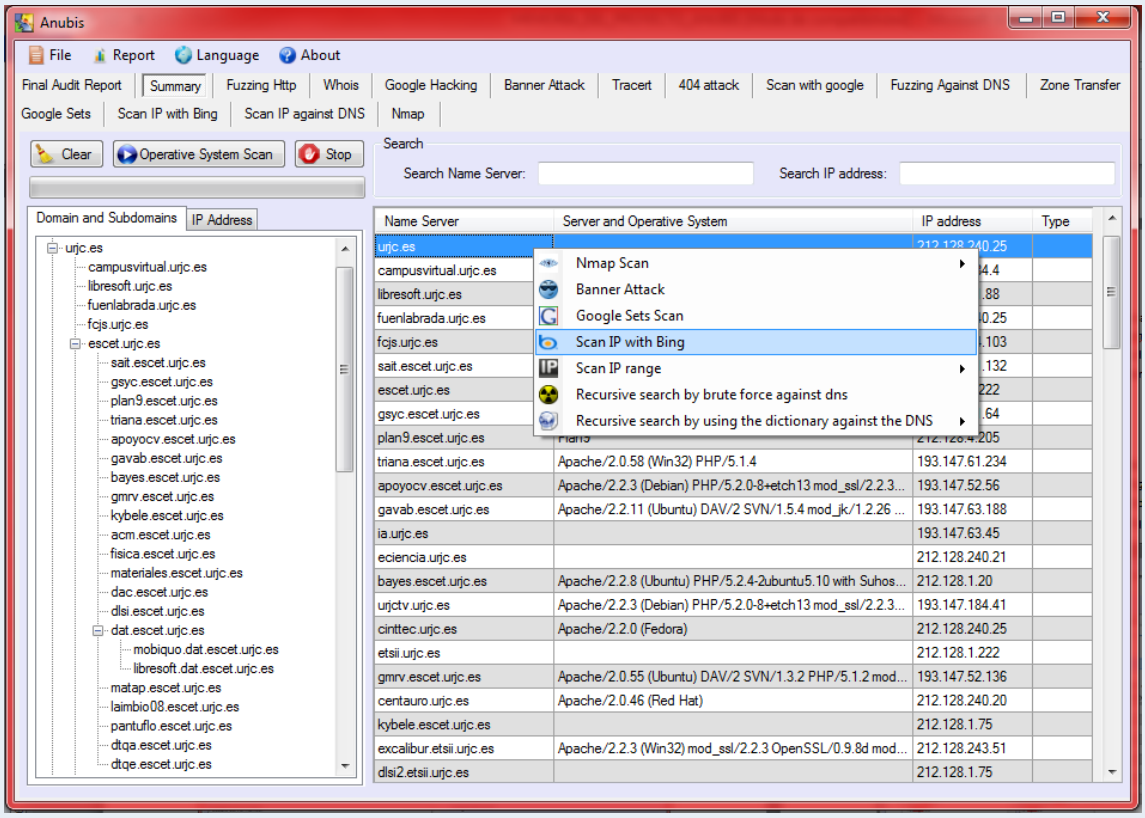
Tras lanzar el escáner hay que desplazarse a la pestaña *Google Set* donde se encontrará el listado de palabras que devuelve *Google Sets* que están relacionadas con el servidor que se le indicó. Si se pulsa el botón *Scan Words*, buscará los servidores que existan que se llamen como alguna de esas palabras.



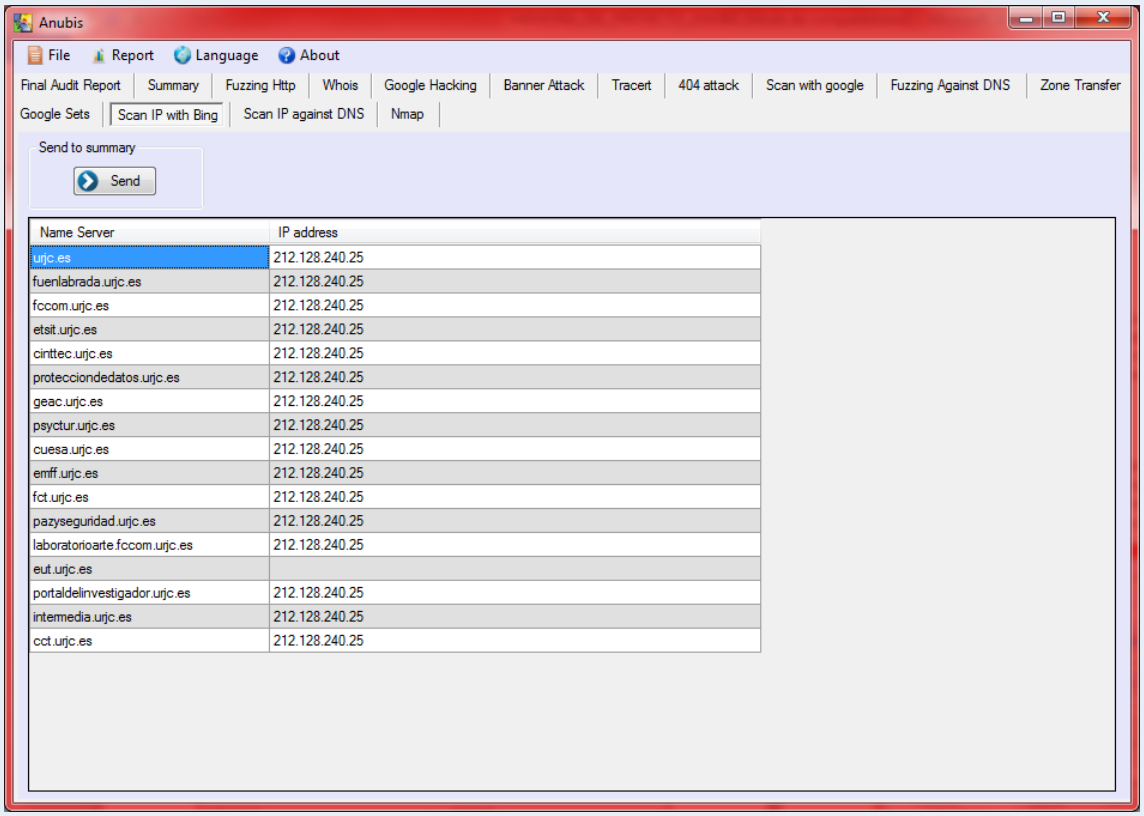
Finalmente se podrán añadir todas las máquinas a la tabla y al árbol que simulará el mapa de la organización de la pestaña *Summary* pulsando *Send*. En esta ocasión Anubis será el encargado de poner una nota de 0 a 10 al estado de la organización dependiendo del número de información obtenida.

Scan IP with Bing

La herramienta *Scan IP with Bing* se lanza de la misma manera que Google Set, y permitirá a través de la búsqueda de *Bing Hacking*, *IP*, encontrar máquinas relacionadas con la IP de la máquina que se le indique. Para lanzar esta herramienta es necesario conocer previamente la IP desde la que se desea realizar el escaneo:



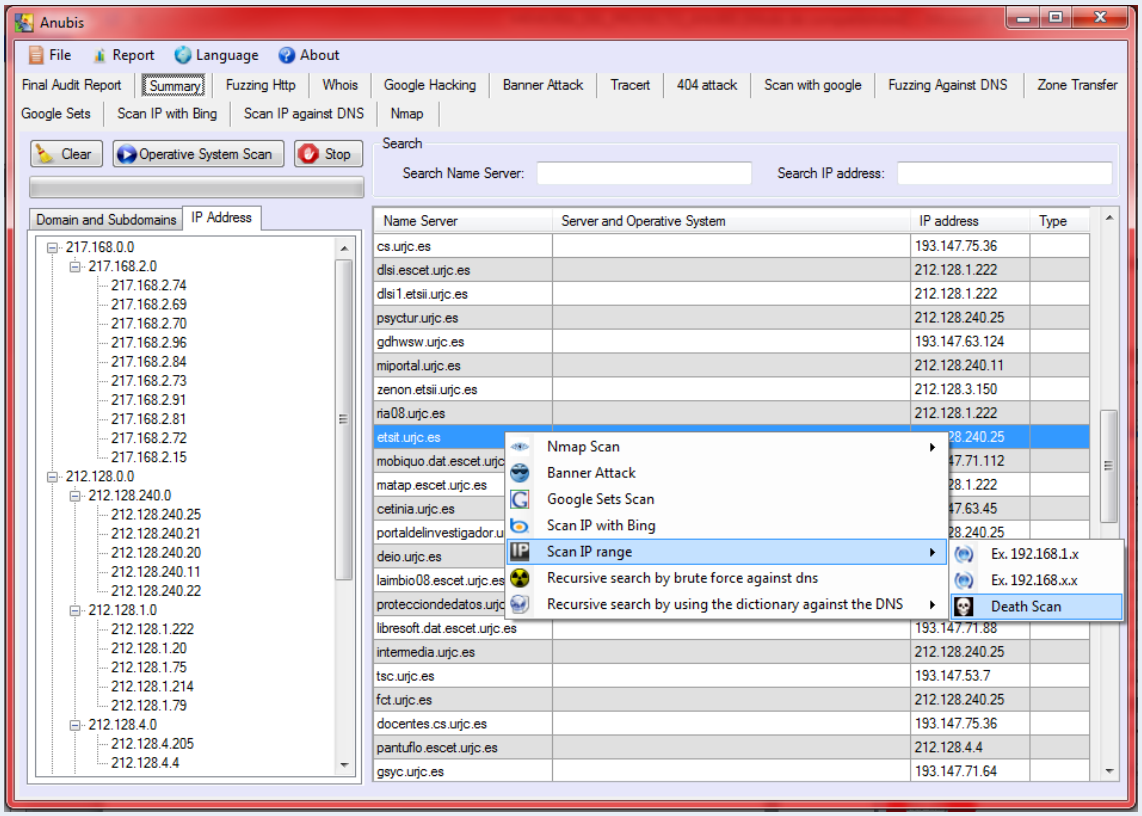
Tras lanzar el escáner hay que desplazarse a la pestaña *Scan IP with Bing* dónde se podrán ver las máquinas encontradas:

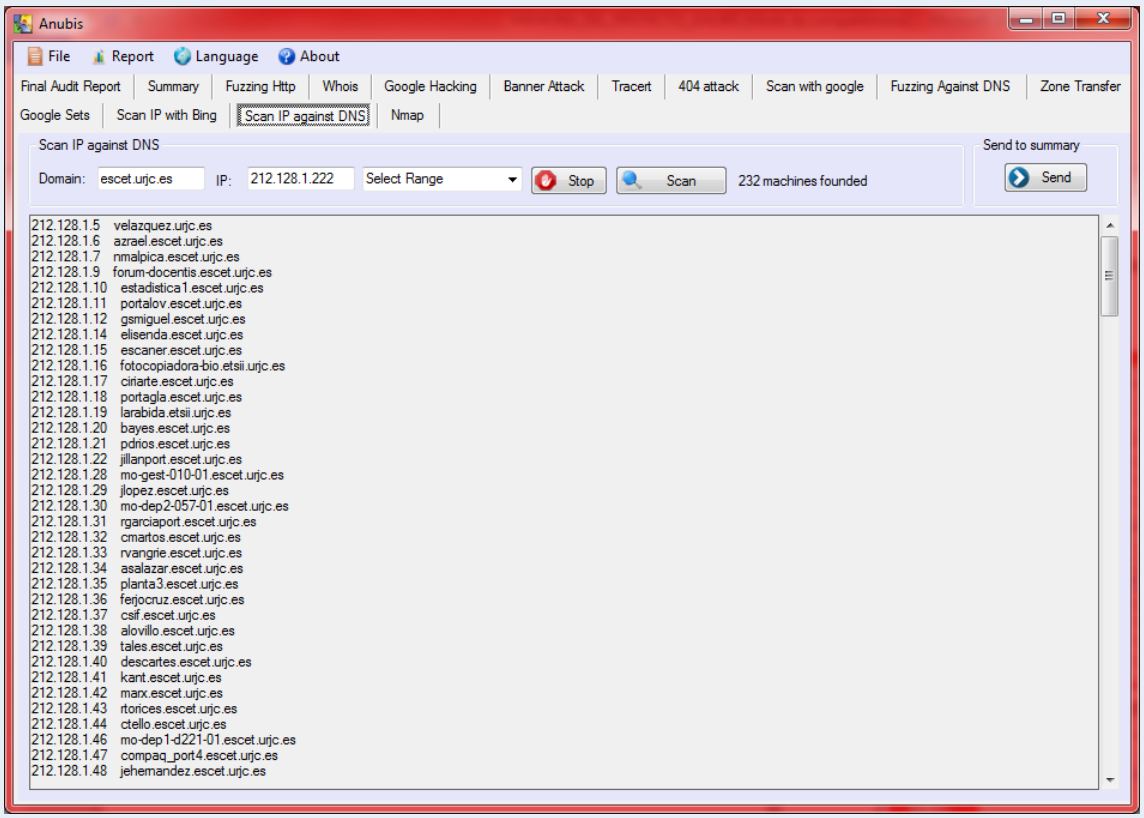


Finalmente podrán ser añadidas todas las máquinas a la tabla y al árbol que simulará el mapa de la organización de la pestaña *Summary* pulsando *Send*. En esta ocasión Anubis será el encargado de poner una nota de 0 a 10 al estado de la organización dependiendo del número de información obtenida.

Scan IP against DNS

Scan IP against DNS permitirá hacer un barrido por IP contra el DNS de tres maneras. La primera y la segunda de ellas lo harán por mascara, escaneando las direcciones IP contiguas a la de la máquina seleccionada con un barrido corto 255 IPs, o con uno largo 65025 IPs. La tercera manera a la que se ha denominado como *Death Scan*, lanzará barridos contra todas las direcciones IP de la tabla *Summary*. Esta última opción peinará la organización obteniendo en caso de que no tenga la organización auditada una buena política de protección en el DNS (por ejemplo, que si se realizan X peticiones en X tiempo se bloqué el acceso a cierta IP) un mapa prácticamente perfecto de la organización. Su eficiencia dependerá de la diversidad de direcciones IP obtenidas en las anteriores fases que se encargaron de rellenar la tabla *Summary* de direcciones IPs internas:



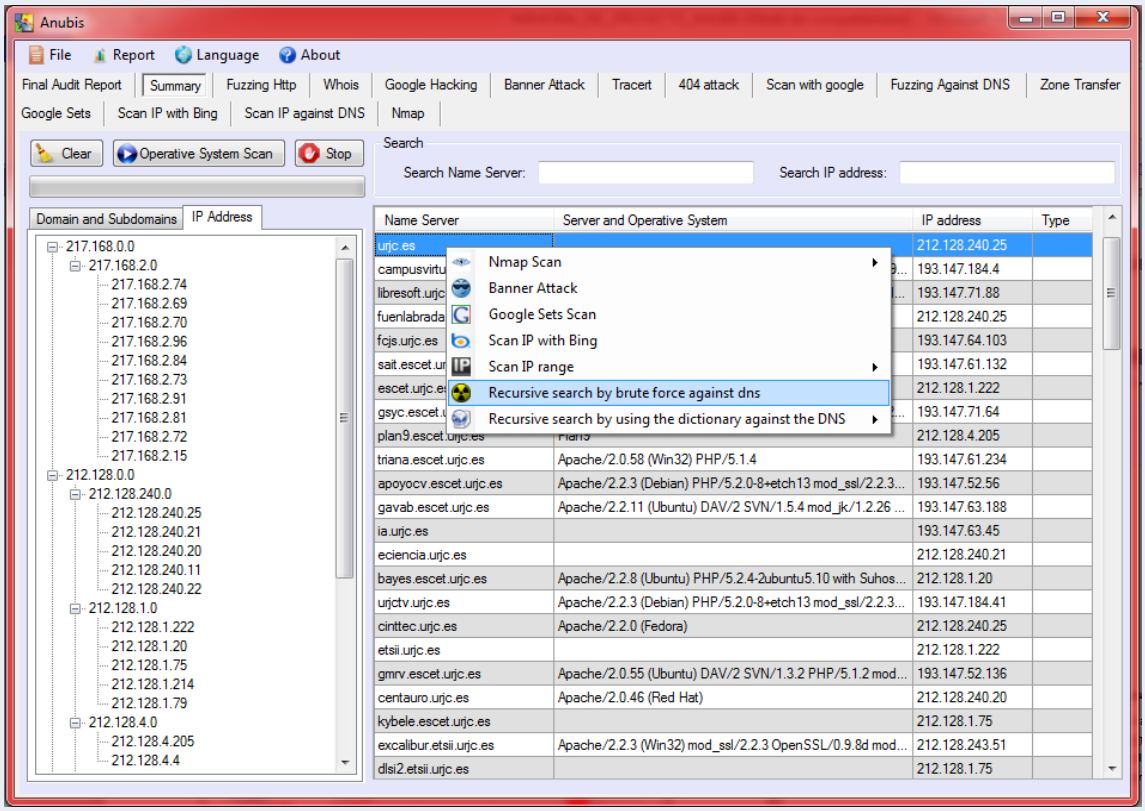


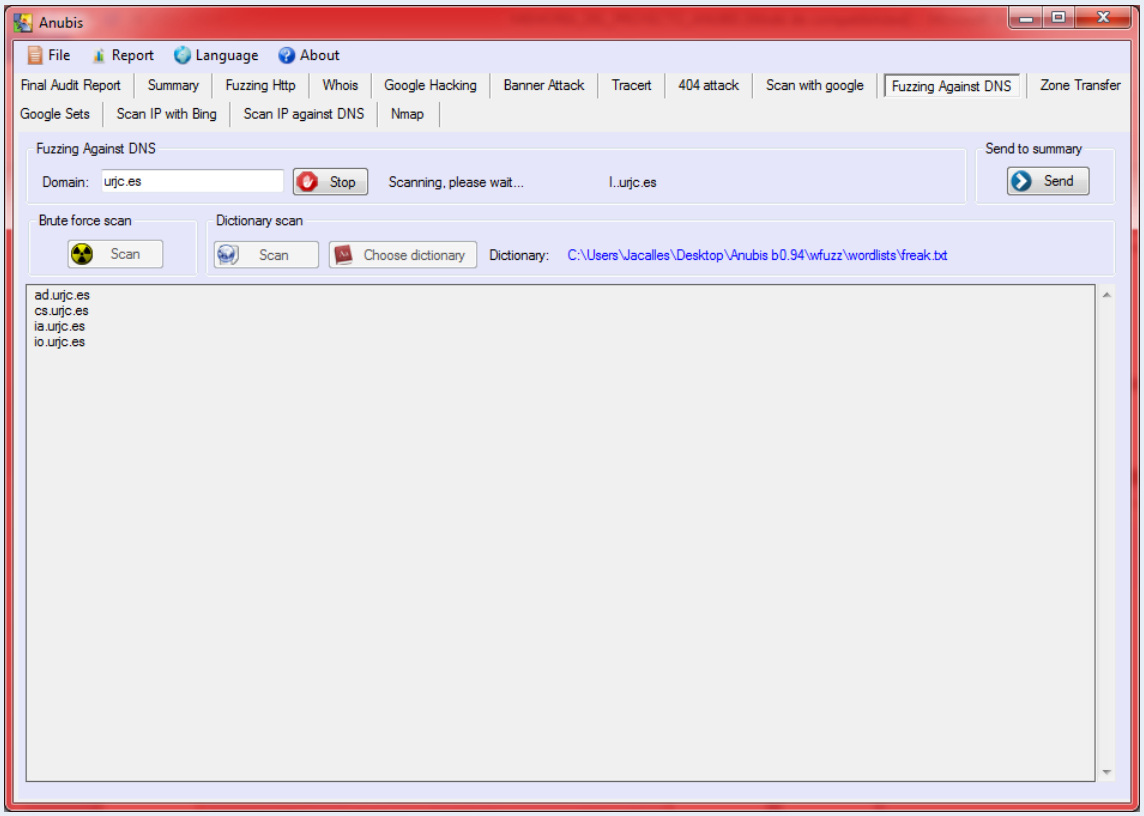
En caso de conocer alguna dirección IP interna del dominio de la organización, éste escaneo también podrá ser lanzado manualmente desde la propia pestaña *Scan IP against DNS*.

Finalmente podrán ser añadidas todas las máquinas a la tabla y al árbol que simulará el mapa de la organización de la pestaña *Summary* pulsando *Send*. En esta ocasión Anubis será el encargado de poner una nota de 0 a 10 al estado de la organización dependiendo del número de información obtenida.

Recursive search by brute force against DNS y Recursive search by using the dictionary against the DNS

Estas dos herramientas permiten lanzar la herramienta *Fuzzing Against DNS* antes comentada contra el subdominio que se le indique. En caso de seleccionar el ataque *Recursive search by using dictionary against the DNS*, previamente se deberá elegir el diccionario con el que se realizará el ataque:

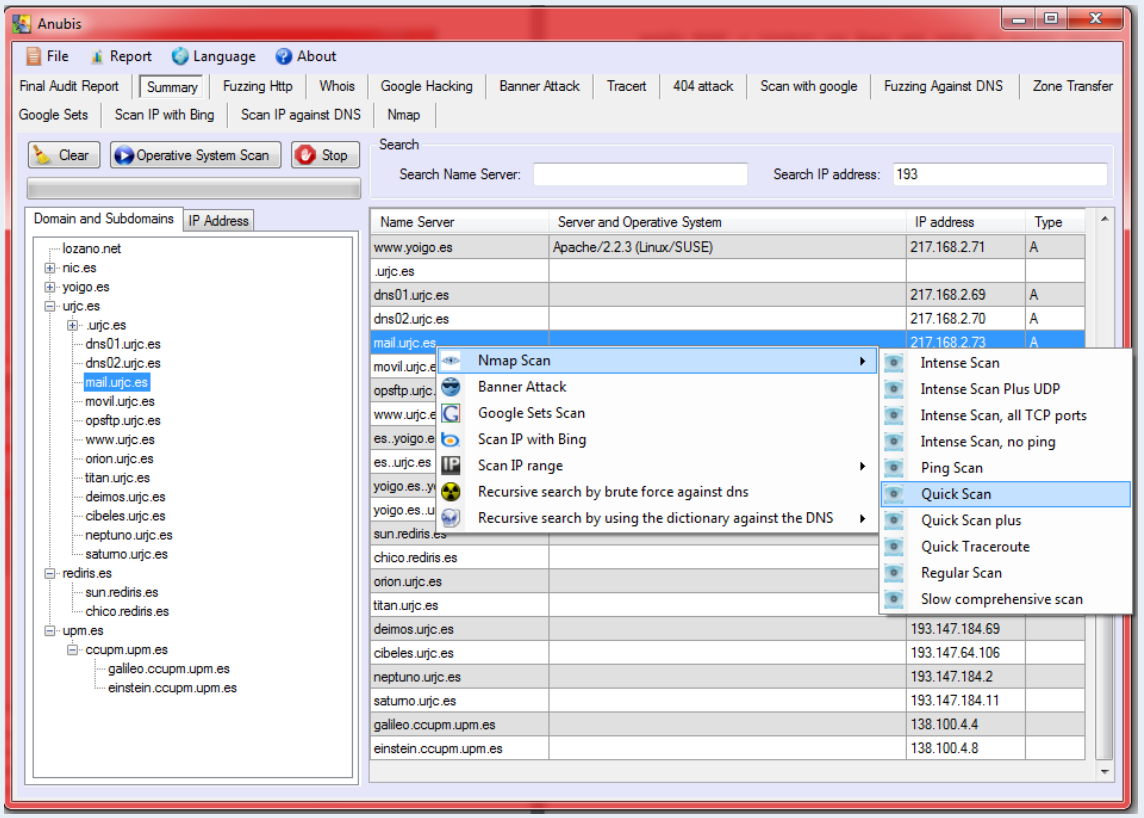


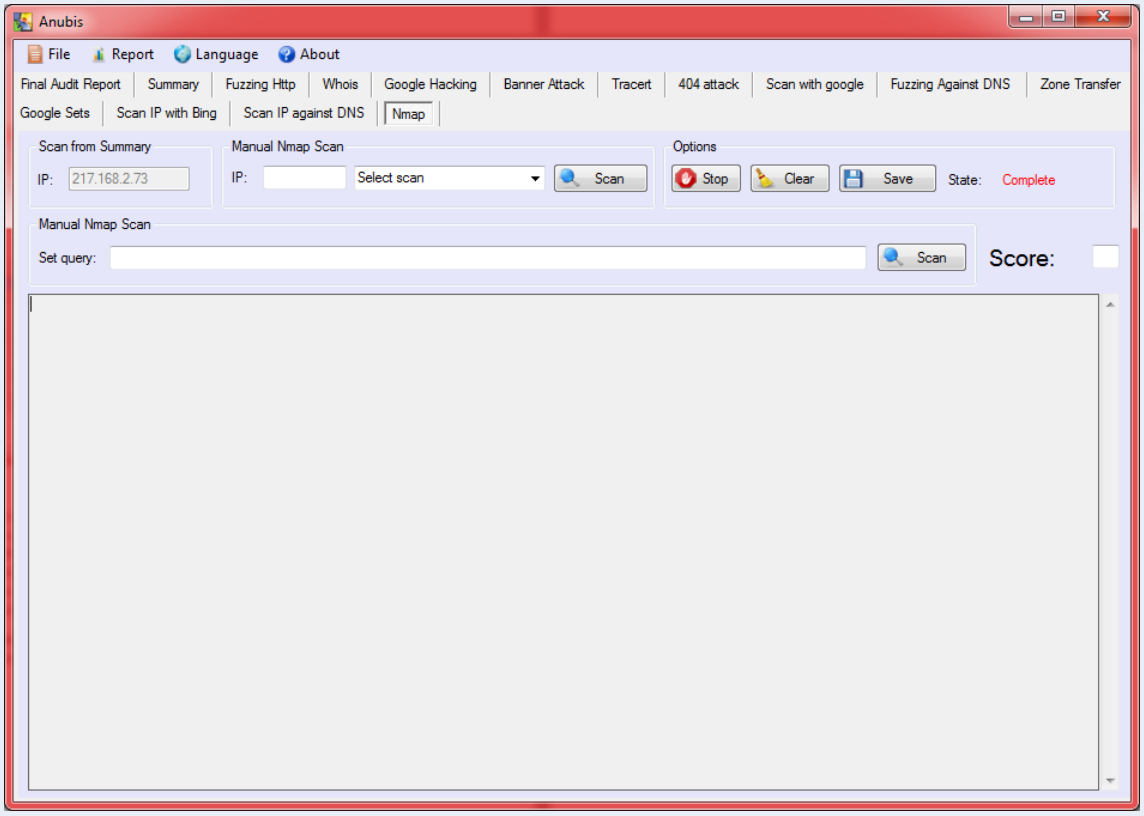


Finalmente se podrán añadir todas las máquinas a la tabla y al árbol que simulará el mapa de la organización de la pestaña *Summary* pulsando *Send*. En esta ocasión Anubis será el encargado de poner una nota de 0 a 10 al estado de la organización dependiendo del número de información obtenida.

NMAP

La última herramienta, *NMAP*, permite lanzar automáticamente uno de sus ataques por defecto a la máquina que se le indique de la tabla *Summary* de una manera cómoda y sencilla, buscando puertos abiertos e intentando averiguar el sistema operativo de la máquina indicada:

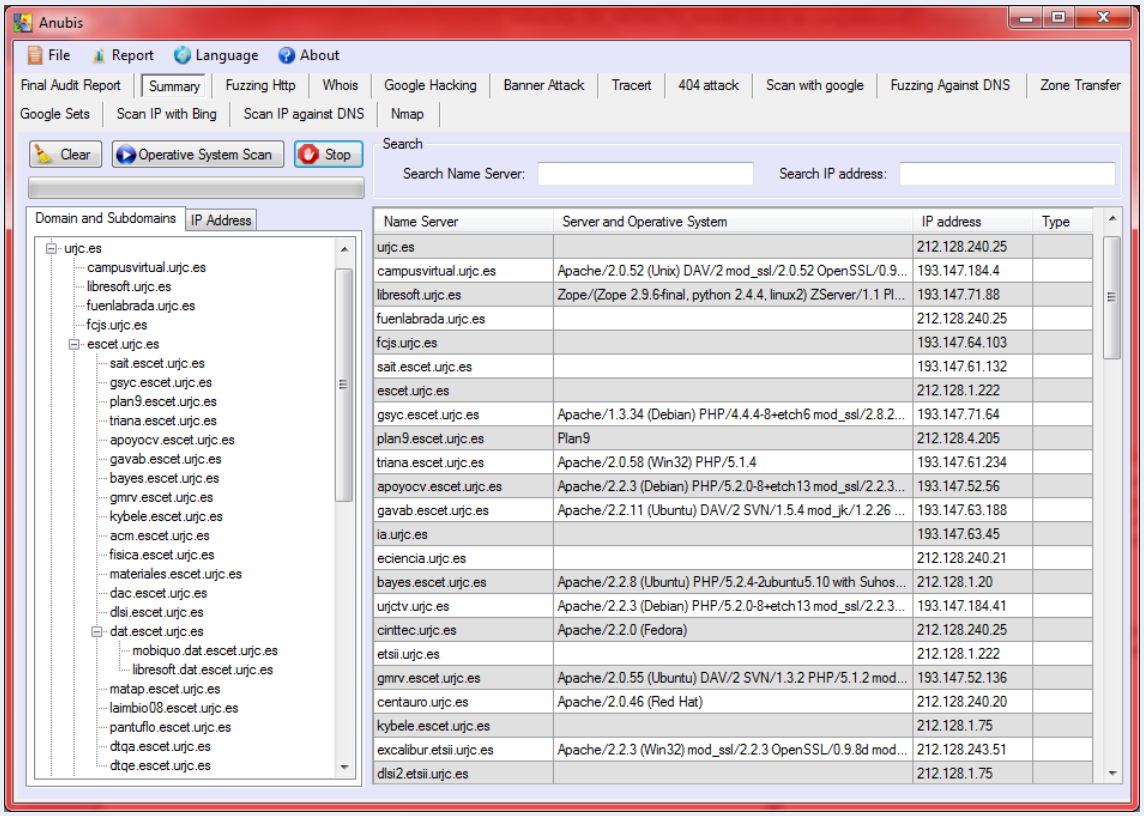




Al igual que en otras herramienta se podrá guardar el reporte en un txt. Por otro lado al igual que en Google Hacking se deberá valorar de 0 a 10 el estado de la organización dependiendo de la información obtenida. Además podrá se lanzado *NMAP* manualmente indicándole una IP y seleccionando el botón *Scan* desde la propia

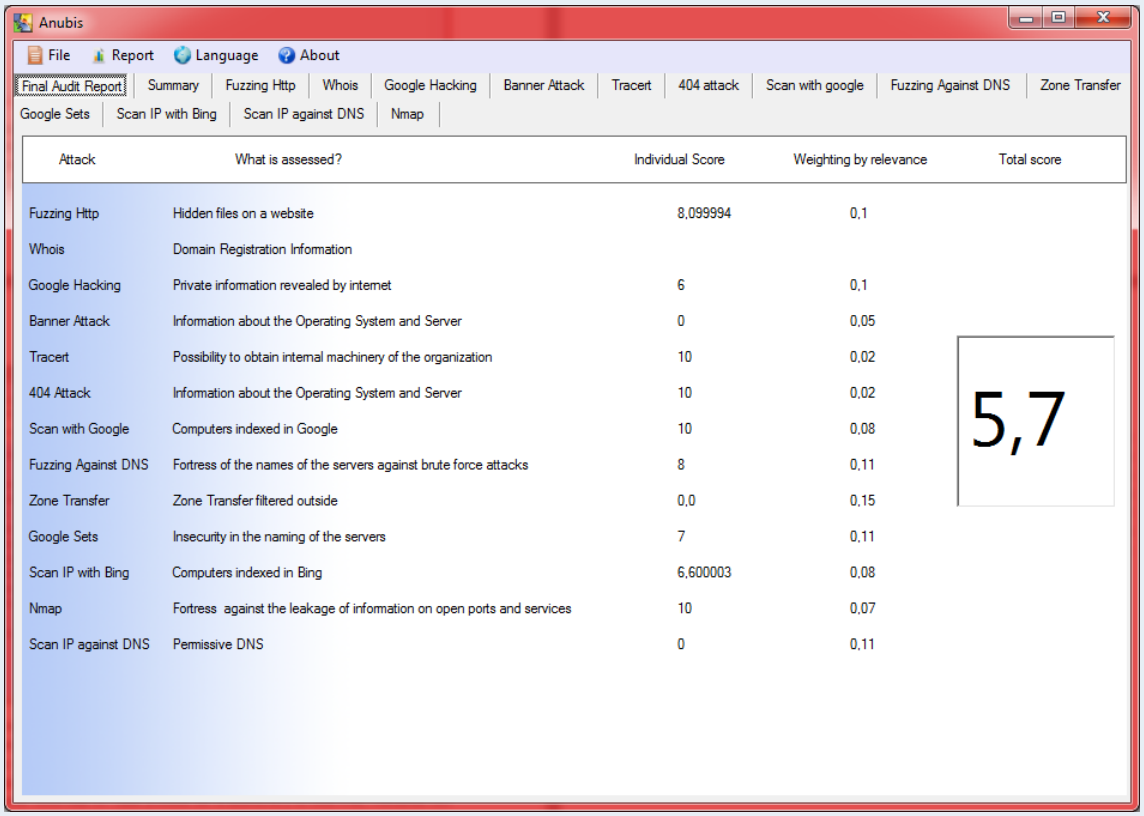
pestaña NMAP, o introducir una Query para realizar un escaneo especial manualmente.

Finalizada la Auditoría en la pestaña *Summary* habrá un mapa completo o casi completo de la red interna de la organización:



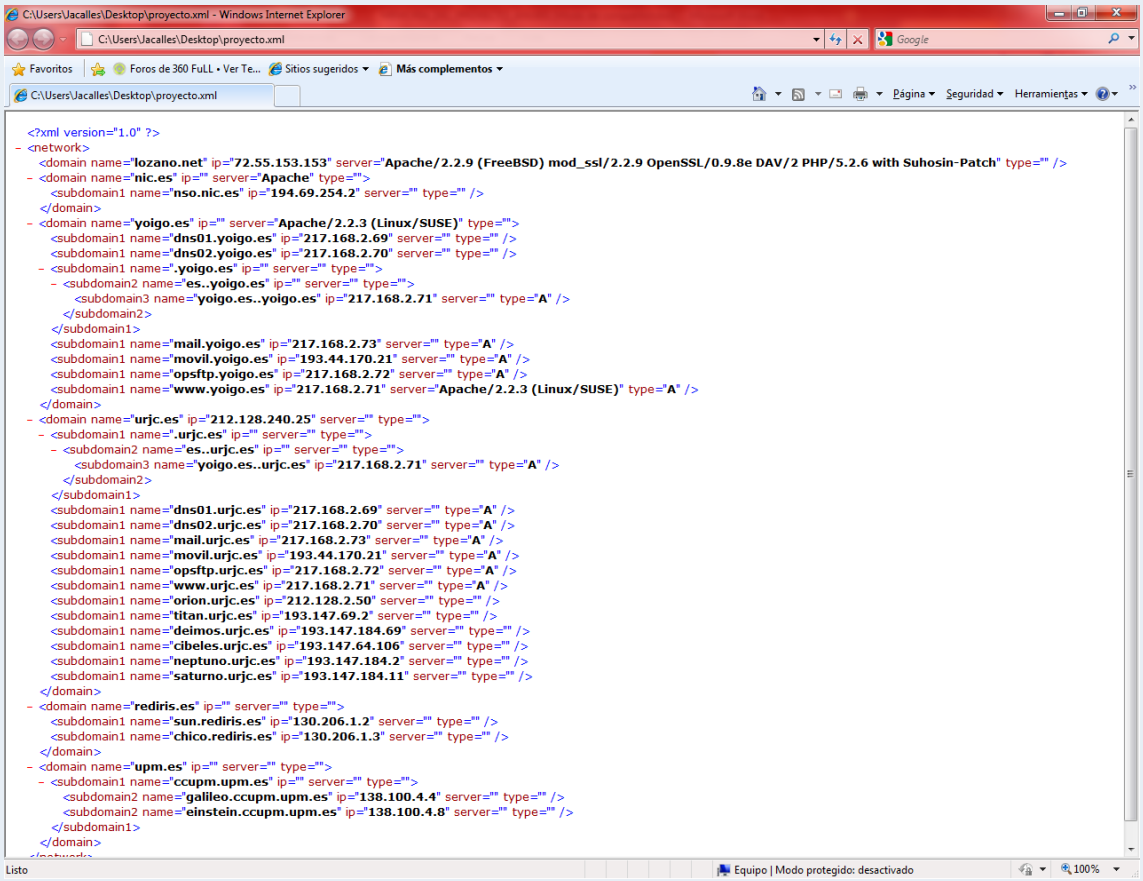
Informe: Final Audit Report

Desde la pestaña *Final Audit Report* se podrán visualizar las notas que ha obtenido la organización en cada sección de la auditoría, valorando globalmente el estado de la organización con una nota de 0 a 10 que se podrá visualizar en la parte derecha del programa:



Una vez finalizada la auditoría se podrá exportar desde el menú Report el mapa de la red obtenido a HTML pulsando el botón *Export network map*. Podrán ser exportadas de igual manera a HTML todas las máquinas obtenidas con sus respectivas IP pulsando el botón *Export computers*. O si se prefiere, exportar a HTML toda la información anterior, junto con las notas obtenidas en cada proceso de la auditoría y la nota final, indicando con colores (rojo, ámbar y verde) el estado de la organización pulsando el botón *Generate Full report*:

Finalmente se podrá guardar el proyecto en formato XML desde la pestaña File, para posteriormente recuperarlo o para ser tratado con otras herramientas.



Wfuzz, Nmap y Whois

Anubis utiliza tres herramientas para realizar algunos escaneos. Estas herramientas se encuentran en la carpeta raíz de Anubis. En caso de querer actualizarlas por versiones más actuales se pueden sustituir sin problemas siempre que se mantenga el mismo nombre de la carpeta raíz de la herramienta, funcionando sin inconvenientes a menos que el fabricante de la herramienta pertinente modifique los comandos que permiten su funcionamiento, en tal caso, se podría mandar un correo a juanantonio.calles@gmail.com explicándole el problema, para ponerle solución en el periodo más corto de tiempo posible.