PaperLab

Hacking Ético

Seguridad Informática

"El automator"

Ciberseguridad

Revisión 4 -11.11

José luis Prado Seoane

A través de este nuevo laboratorio práctico desarrollaremos una nueva vía de captación de información para la determinación objetiva de nuevas IP´s relacionadas con un objetivo. En primer lugar aislaremos y modificaremos el Resolver del paper.elbuscador* (Resolverdb3.py --> Resolverdb3_dic.py) para únicamente la determinación por diccionario el cuál, recordemos fue conformado a través de diferentes fuentes de Ingeniería Social (nombreserv.txt), y modificaremos el código para que nos permita la recepción de parámetros en la entrada del Script para la automatización del proceso de captación. A continuación, retocaremos un poco el Bind (2ghoww45.db) introduciendo un número mayor de máquinas visibles en concordancia con el reverse, que le permita ver la técnica de ejemplo con mayor claridad de igual manera, retocaremos el diccionario (nombreserv.txt) que nos servirá como resolución reduciendo su tamaño. Reinicie Bind después de realizar los cambios.

Alimentaremos el diccionario con un nuevo canal de información más automatizado a través de fuentes de información abiertas o públicas y recuerde, que en su continua búsqueda relacionada con la infraestructura de su objetivo a través de la Red un atacante cualificado, tendrá en cuenta sin lugar a dudas las mismas, estas podrían ser Google, Bing (no olvide que estos sistemas han sido diseñados únicamente con un propósito comercial o de búsqueda de negocio algo que deberá tener en cuenta en función del ámbito que desempeñe en su trabajo, no es lo mismo que desarrolle su función como Pentester que sea un analista de Información, de Ciberseguridad o Ciberdefensa que sí lo deberá tener muy presente) o Shodan, entre otras, parametrizando todo mediante caracteres especiales de búsquedas específicas y precisas sobre objetivos bien definidos que bien empleados y focalizados en cachés Web le "garantizarán un anonimato" (sin imágenes, utilice al final de la consulta: &strip=1) eficaz, por no decir que lo acompañe de otras medidas de ocultación además, buscará todo tipo de información disponible no indexada por Google y otros buscadores en el DeepWeb relacionada con el objetivo a través de aplicaciones específicas o sus propias herramientas de búsqueda, algo que seguro utilizará.

resolverdb3_dic.py

```
#!/usr/bin/env python
# -*- coding: latin-1 -*-
#Versión:Python 2.7.6
#Check 24/05/2014
#Sistema:Backtrack5_release_10.04
#Kernel:linux 2.6.38
#Puede copiar,modificar y publicar este codigo en el medio que desee #haciendo referencia de origen al autor del mismo.
#Utilice el mismo con responsabilidad en entornos seguros y controlables

import os,sys,commands

def resolverhosts():
    origen = open('nombreserv.txt','r')
    filtradodirecto = open('filtradodirecto.txt','w+')
    maquinas = origen.readlines()

    for host in maquinas[:-1]:
      resolucion = os.system ("host %s.%s > /dev/null" % (host[0:-1],dominio))
      if ( resolucion == 0 ) :
```

```
                resultado = commands.getoutput("host %s.%s" % (host[0:-1],dominio))
                filtradodirecto.write(resultado.replace("%s.%s has address " % (host[0:-1],dominio),"") + "\n")
                print resultado.replace("%s.%s has address " % (host[0:-1],dominio),"")

    origen.close()
    filtradodirecto.close()
    return;

print ""
print ("Versión: Free")
print ("Check 07/04/2014")
print ""
print ("Esta herramienta es didáctica y forma parte del libro ")
print ("y curso avanzado de Hacking++ de Seguridad Informática ")
print ""
print ("[Herramienta sin optimizar para estudio]")
print ""
print ("ANÁLISIS POR DICCIONARIO...")
print ("**************************")
print ""

if len(sys.argv) >= 2:
  dominio = sys.argv[1]
  resolverhosts();
else:
  print "Error: especifica el dominio como argumento de resolución"
  print ""
```

2ghoww45.db

```
;
; BIND centraltermica.lan
;
@ IN SOA centraltermica.lan. root.centraltermica.lan. (
                1 ; Serial
                604800 ; Refresh
                86400 ; Retry
                2419200 ; Expire
                604800 ) ; Default TTL
                IN NS ns1.centraltermica.lan.
                IN MX 5 mail1.centraltermica.lan.
                IN MX 10 mail2.centraltermica.lan.
                IN MX 20 mail3.centraltermica.lan.
ns1 IN A 192.168.1.37 ← (Establezca aquí la IP asignada a su tarjeta de red)
ftp IN A 192.168.1.100
administracion IN A 192.168.1.101
contabilidad IN A 192.168.1.102
facturacion IN A 192.168.1.103
backup IN A 192.168.1.104
fichastecnicas IN A 192.168.1.105
mail1 IN A 192.168.1.106
mail2 IN A 192.168.1.107
mail3 IN A 192.168.1.108
login IN A 192.168.1.109
router IN A 192.168.1.200
www IN A 192.168.1.250
contactores IN A 192.168.1.220
valvulas IN A 192.168.1.221
bypass IN A 192.168.1.222
accesos IN A 192.168.1.225
termicos IN A 129.168.1.226
gestion IN A 129.168.1.228
suministro IN A 129.168.1.230
nodo2 IN A 129.168.1.231
apagado IN A 129.168.1.232
alarmas IN A 129.168.1.234
perimetros IN A 129.168.1.235
personal IN A 129.168.1.236
mandoycontrol IN A 129.168.1.239
partnumbers IN A 129.168.1.242
resets IN A 129.168.1.246
```

nombreserv.txt

```
ns1
ns2
ns3
ns4
www
www2
smtp
jefe
administracion
contabilidad
facturacion
remoto
backup
fire
virtual
```

Centraremos nuestro estudio en Google , - *de las múltiples "fuentes abiertas" de las que disponemos en el ciclo de captación o recopilación de información* - , como recurso abierto disponible y en la finalidad principal de su uso para el análisis o exploración de la infraestructura de un objetivo tal y como lo haría un atacante. Le recuerdo que con independencia de la finalidad de este paper podrá utilizar esta técnica para obtener desde Logeados de los sistemas, Fingers de los sistemas Operativos existentes, configuraciones, DB´s, errores asociados a las tecnologías implementadas, claves y accesos, etc.-, los cuales algunos de ellos servirán como complemento a una exploración de Red. Sólo las destreza y la experiencia podrá límites a esta búsqueda de información.

A continuación le mostraré algunos de los "comandos" y parámetros básicos que se utilizarán en el proceso de captación de información pública (Google Hacking) :

(**Practica 1**): Documéntese por cuenta propia. En Internet podrá encontrar toda la información que necesite al respecto y no olvide, la utilización de foros especializados que le ayudarán en esta tarea.

Principales parámetros

Comillas dobles " "	Permite buscar frases exactas	"Windows Xp"
Operadores lógicos or / and / Not	(or = ||) permite añadir varias condiciones (and = &&) permite evaluar si se cumplen las dos condiciones de búsqueda	ext:txt || ext:txt intext:1234qwerty ext:txt || ext:txt intext:1234qwerty && intext: centraltermica
Operadores (+) y (-)	(+) incluye o admite (-) excluye u omite	centraltermica – gas (busca por la palabra centraltermica pero excluye aquellas Webs con la palabra gas)
Asterisco (*)	Es un comodín. Cualquier palabra, pero una sola	Central*
Punto (.)	Es otro comodín. Cualquier palabra, una sola o muchas	
link:	Busca en páginas que tienen un link a una determinada Web	Link:www.centraltermica.net
ext:	Busca por extensión de archivo. Tiene que ir acompañado de otros parámetros de búsqueda para que sea efectivo	ext:txt inurl:hosts
Filetype:	Similar al parámetro anterior pero extensible a otros formatos como: pdf,docx,xml,doc…	filetype:txt inurl:hosts
intitle/allintitle	intitle: Devuelve los resultados de aquellas URL´s que contengan al menos una de las palabras especificadas en los "títulos de las páginas" allintitle: Devuelve los resultados de aquellas URL´s que contengan todas las palabras especificadas en los "títulos de las páginas"	intitle:"index of /" allintitle:"index of /admin/"
inurl/allinurl	inurl: Devuelve los resultados de aquellas URL´s que contengan al menos una de las palabras especificadas allinurl : Devuelve los resultados de aquellas URL´s que contengan todas las palabras especificadas	inurl:"MultiCameraFrame?Mode=Motion" allinurl:"hacking ético"
intext/allintext	intext: Devuelve los resultados de aquellas URL´s que contengan al menos una de las palabras especificadas dentro del cuerpo de la página	Intext:"usando clave"

	allintext: Devuelve los resultados de aquellas URL´s que contengan todas las palabras especificadas dentro del cuerpo de la página	
cache	Uno de los parámetros más importantes. Permite una especie de “anonimato” a un atacante al no acceder directamente al sitio en Internet evitando cualquier tipo de logeado asociado.	cache:cursohackingetico.com
info	Devuelve información sobre el dominio especificado, nos mostrará una serie de opciones relacionadas con el caché, páginas similares, Webs con enlaces al site, páginas del sitio o páginas Web dónde aparezca el termino solicitado.	info:cursohackingetico.com
site	Permite reducir la búsqueda de uno o varios dominios especificados inclusive directorios	site:cursohackingetico.com site:cursohackingetico.com/temario
inanchor/allinanchor	Devuelve aquellas páginas que contienen enlaces con el anchor especificados.	

En primer lugar realizaremos la instalación del navegador para consola (Lynx) que nos permitirá efectuar consultas parametrizadas y su tratamiento o análisis posterior, que sumado a un proceso de anonimación podremos realizar dichas consultas con "seguridad". Podrá utilizar igualmente otros navegadores similares existentes, lo importante es que se quede con la idea y técnicas que se desarrollarán. También podría implementar codificación utilizando el API de Google utilizando Python, el inconveniente es que necesitará una licencia (free) que deberá establecer en el Script que utilice para la búsqueda en Internet por lo que no será anónimo en su trabajo, algo que en función de su ámbito de actuación, puede llegar a no ser deseable en algunos casos como; Ciberinvestigaciones, Ciberinteligencia, investigaciones periodísticas, investigaciones de los cuerpos de seguridad o cualquier otro tipo de investigación similar.

Una vez realizada la instalación ejecutaremos diferentes consultas básicas para entender la técnica, no olvide que si realiza consultas automatizadas sobre un mismo dominio Google lo detectará y le filtrará (desde su navegador gráfico), deberá actuar modulando el tiempo, alternando los diferentes "actores" implicados en la búsqueda asociados al dominio y un largo de técnicas que seguro por cuenta propia desarrollará.

Banner de aviso

Para continuar, introduce los caracteres que aparecen a continuación:
...
Acerca de esta página

Nuestros sistemas han detectado tráfico inusual procedente de tu red de ordenadores. En esta página se comprueba si eres tú quien envía las solicitudes en lugar de un robot. ¿A qué se debe esto?

Dirección IP: xx.xx.xxx.xxx
Hora: 2012-02-14T08:33:30Z
URL:https://www.google.es/search?output=search&sclient=psy-ab&q=site:www.xxxxxx.com+intext:%22%C3%A1mbitos+perimetrales%22&oq=site:www.xxxxxx.com+intext:%22%C3%A1mbitos+perimetrales%22&gs_l=hp.12...36.38.0.6098.2..0.972.113.0j1j6-1.2....1c.2.43.psy-ab..2.0.0.0.fpgJK4ZZ3LE&pbx=1&bav=bv.6933%.....

Finalmente, continuando con el propósito del paper y en la línea de los Labs anteriores nos centraremos en la captación de datos del dominio simulado "centraltermica.lan" asumiendo para su evaluación las mismas máquinas y servidores presentadas con anterioridad y que el mismo es público y accesible desde Internet. Para ello codificaremos para analizar y filtrar la información obtenida a través de un Script que nos permitirá determinar o ampliar esas máquinas o servidores que buscamos complementando al diccionario existente, pero esta vez, Google lo hará por nosotros de una forma automatizada. El marco de trabajo es infinito y sólo sus conocimientos en programación e imaginación serán su límite. Las técnicas presentadas le servirán únicamente

como base, pero le aseguro que le abrirán la mente y despertarán su curiosidad, piedra angular del Hacking más apasionante que al servicio de la seguridad se convierte en un valor añadido.

(**Recuerde:** actúe con responsabilidad, lo importante es que aprenda esta y otras técnicas.)

Empezaremos instalando el navegador Lynx para consola, - *podrá utilizar el que quiera pero para el ejemplo de la siguiente técnica será el que utilizaremos* -.

```
root@lab:/# apt-get install lynx
...
```

Ejemplos por consola utilizando como Dumpeado a Lynx

```
root@lab:/#
lynx -dump http://www.google.es/search?q=Password+crackers+site%3Acentraltermica.lan

root@lab:/#
lynx -dump http://www.google.es/search?q=Password+crackers+site%3Acentraltermica.lan+-site%3Aforo.centraltermica.lan

root@lab:/#
lynx -dump http://www.google.es/search?q=site%3Awww.centraltermica.lan+intext%3A"ámbitos+perimetrales"

root@lab:/#
lynx -dump http://www.google.es/search?q=site%3Awww.centraltermica.lan+ext%3Apdf
```

La técnica que se le presentará es muy sencilla, pero a la vez muy eficaz o práctica, para ello mecanizaremos una consulta manual y en el tiempo para no despertar la "curiosidad y el cabreo del navegador" dirigida a Google especificando nuestro dominio de búsqueda y desarrollando posteriormente un Script que nos permita formatear la salida obtenida en la búsqueda de máquinas o servidores asociados al mismo. Imagínese que automatiza consultas a diferentes dominios internamente en un Script, las modula en tiempo, "Switchea" las mismas para no establecer patrones lineales de detección, lo anonimiza todo, establece un server dedicado que recopile dichos datos en un periodo extenso (días o meses, i/ años) y que sirva como maestro a una serie de máquinas locales o externas públicas "onionizadas" a modo de Pull, ¿Le suena de algo?.

(*mire el Help de Lynx y verá las múltiples opciones de que dispone como por ejemplo el Store de cookies, tiempos y un amplio abanico de parámetros para conformar su consulta*)

A continuación estableceremos una consulta básica en busca de esta información, no olvide que esto es un ejemplo y que el límite está en usted.

(**Practica 1**): Experimente con diferentes consultas utilizando Google Hacking y formateando a su gusto las diferentes salidas. Concatene diferentes tareas de una forma manual a través de "sleeps" de una forma automatizada lineal y comprenderá mejor la potencia de esta técnica.

Al ejecutar la consulta a través de Lynx se "dumpeará" la salida hacia un file (dump_gh.txt) que nos permitirá obtener cadenas de datos en la que se encuentran aquellos nombres o máquinas que Google ha encontrado asociados al dominio. El formateo lo podrá hacer en bruto secuenciando el dominio o a través de las "References", es indiferente, particularmente en esta búsqueda prefiero References ya que reducirá el código del Script y es más directo, para ello introduzca "-listonly" en la cadena de consulta.

```
root@lab:/#cd /libro/modulo1      (vaya al directorio de trabajo del módulo 1)

root@lab:/libro/modulo1#
lynx -dump http://www.google.es/search?q=site%3Acentraltermica.lan > dump_gh.txt
```

dump_gh.txt (búsqueda general)

(Se han omitido algunas partes del volcado para su análisis)

```
Búsqueda [1]Imágenes [2]Maps [3]Play [4]YouTube [5]Noticias [6]Gmail
[7]Drive [8]Más »

. . .

[15]Central Térmica ES | Servicios y Recursos públicos
```

Nuestra misión es proporcionarle la información que necesite sobre nuestras actividades y nuestro compromiso con el medio ambiente
www.centraltermica.lan/ - 110k - [16]En caché - [17]Páginas similares

. . .

References

1. http://www.google.es/search?q=site:centraltermica.lan&um=1&ie=UTF
8&hl=es&tcm=isch&source=ag&sa=N&tab=wi
2. http://maps.google.es/maps?q=site:centraltermica.lan&um=1&ie=UTF-8&hl=es&sa=N&tab=wl
...
21. http://www.google.es/url?q=http://central.centraltermica.lan/&sa=U&ei=ylJ-U_KyL-
ic0AXvxxxxxA&ved=0Cxxxxxxx&usg=AFQjCNExxxxxxxxxxxxq0e0GHxxxxxxxDg
. . .

root@lab:~/dumpersgh#
lynx -dump -listonly -nonumbers http://www.google.es/search?q=site%3Acentraltermica.lan > dump_gh.txt

(**Practica 2**): La salida de ambas opciones le muestra el primer Dump_file (primeras búsquedas de Google) por lo que le propongo como práctica para reforzar la técnica y la amplitud de la misma en la recopilación de datos que realice la búsqueda de todos los files (páginas) que Google le devuelva hacia el mismo archivo receptor. Consejo para su resolución: Lynx le permitirá aceptar todas las Cookies relacionadas (por parámetro) así como, asociar un archivo (Script) para automatizar el proceso.

dump_gh.txt (búsqueda References)
(Se han dumpeado de Lynx varias páginas de resolución de Google)

References

http://www.google.es/url?q=http://www.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OPD00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://www.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://www.centraltermica.lan/&hl=
http://www.google.es/url?q=http://remoto2.centraltermica.lan/&sa=U&ei=ai6CUnYCaqa0AWSkIHYDg&ved=0CBsQFjAB&usg=AFQjCNFr_14ahi0NTbJHLObesafZczvZcA
http://webcache.googleusercontent.com/search?q=cache:jZt5LPPCHnYJ:http://remoto2.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://remoto2.centraltermica.lan/&hl=
http://www.google.es/url?q=http://resets.centraltermica.lan/&sa=U&ei=ai6CUnYCaqa0AWSkIHYDg&ved=0CBwQFjAC&usg=AFQjCNEOKzI1rrIgumbIzv_LzbRONGQ6g
http://webcache.googleusercontent.com/search?q=cache:INUyc1dLc_oJ:http://resets.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://resets.centraltermica.lan/&hl=
http://www.google.es/url?q=http://backupconfig.centraltermica.lan/&sa=U&ei=ai6CUnYCaqa0AWSkIHYDg&ved=0CB0QFjAD&usg=AFQjCNHfC1WDyPKFVZ9Ro1g323G4W8eRFw
http://webcache.googleusercontent.com/search?q=cache:ybK6v2PnnC4J:http://backupconfig.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://backupconfig.centraltermica.lan/&hl=
http://www.google.es/url?q=http://partnumbers.centraltermica.lan&sa=U&ei=ai6CUnYCaqa0AWSkIHYDg&ved=0CB4QFjAE&usg=AFQjCNE7hRgrggTHkOlAOWbBvqQNNUKOtw
http://webcache.googleusercontent.com/search?q=cache:bjfVFCo9hIYJ:http://partnumbers.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://partnumbers.centraltermica.lan/&hl=
http://www.google.es/url?q=http://micros.centraltermica.lan/siem/&sa=U&ei=ai6CUnYCaqa0AWSkIHYDg&ved=0CB8QFjAF&usg=AFQjCNHo5in3cfaBLbHVT7JYggayh6fUgQ
http://webcache.googleusercontent.com/search?q=cache:f3f_O5_k74J:http://micros.centraltermica.lan/siem/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://micros.centraltermica.lan/siem/&hl=
http://www.google.es/url?q=http://comunicaciones.centraltermica.lan/wifi/&sa=U&ei=ai6CUnYCaqa0AWSkIHYDg&ved=0CCAQFjAG&usg=AFQjCNETLm1YOKHWbRcDZjN_0NjwRHyCXQ
http://webcache.googleusercontent.com/search?q=cache:swsRDyDtTJQJ:http://comunicaciones.centraltermica.lan/wifi/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://comunicaciones.centraltermica.lan/wifi/&hl=
http://www.google.es/url?q=http://mandoycontrol.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OPD00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://mandoycontrol.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://mandoycontrol.centraltermica.lan/&hl=
http://www.google.es/url?q=http://central.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OPD00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://central.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://central.centraltermica.lan/&hl=

http://www.google.es/url?q=http://motores.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OPD00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://motores.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://motores.centraltermica.lan/&hl=
http://www.google.es/url?q=http://personal.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OPD00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://personal.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://personal.centraltermica.lan/&hl=
http://www.google.es/url?q=http://perimetros.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OPD00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://perimetros.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://perimetros.centraltermica.lan/&hl=
http://www.google.es/url?q=http://alarmas.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OPD00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://alarmas.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://alarmas.centraltermica.lan/&hl=
http://www.google.es/url?q=http://apagado.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OPD00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://apagado.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://apagado.centraltermica.lan/&hl=
http://www.google.es/url?q=http://nodo2.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OPD00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://nodo2.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://nodo2.centraltermica.lan/&hl=
http://www.google.es/url?q=http://gestion.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OPD00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://gestion.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://gestion.centraltermica.lan/&hl=
http://www.google.es/url?q=http://accesos.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OPD00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://accesos.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://accesos.centraltermica.lan/&hl=
http://www.google.es/url?q=http://bypass.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OPD00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://bypass.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://bypass.centraltermica.lan/&hl=
http://www.google.es/url?q=http://valvulas.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OPD00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://valvulas.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://valvulas.centraltermica.lan/&hl=
http://www.google.es/url?q=http://contactores.centraltermica.lan/&sa=U&ei=aiCU-nYCaqved=0CBoQFjAA&usg=AFQjCgH3OP-D00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://contactores.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk http://www.google.es/search?q=related:http://contactores.centraltermica.lan/&hl=
http://www.google.es/url?q=http://router.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OP-D00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://router.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://router.centraltermica.lan/&hl=
http://www.google.es/url?q=http://login.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OP-D00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://login.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://login.centraltermica.lan/&hl=
http://www.google.es/url?q=http://mail3.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OP-D00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://mail3.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://mail3.centraltermica.lan/&hl=
http://www.google.es/url?q=http://backup.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OP-D00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://backup.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk
http://www.google.es/search?q=related:http://backup.centraltermica.lan/&hl=
http://www.google.es/url?q=http://administracion.centraltermica.lan/&sa=U&ei=aiCUnYCaqved=0CBoQFjAA&usg=AFQjCgH3OP-D00lv_fkg

http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://administracion.centraltermica.lan/+site%3Acentraltermica.lan&hl=&ct=clnk http://www.google.es/search?q=related:http://administracion.centraltermica.lan/&hl=

Una vez obtenido el "dumpeado" al archivo receptor (dump_gh.txt), realizaremos el Parser (parser_url_gh.py) en Python y lo ejecutaremos contra el mismo, lo que le permitirá filtrar y sintetizar la información obtenida contra el dominio (centraltermica.lan) en la búsqueda de máquinas asociadas (dump_gh_filter.txt). Una vez obtenido el filtrado compararemos el resultado con el diccionario (dump_gh_filter.txt <--> nombreserv.txt) añadiendo más nombres de máquinas al mismo en la búsqueda de sus IP´s correspondientes, el objetivo final de todo atacante. Esta es una de las múltiples técnicas que podrá desarrollar por lo que no dude en experimentar con otras ideas o implementaciones que se le puedan ocurrir.

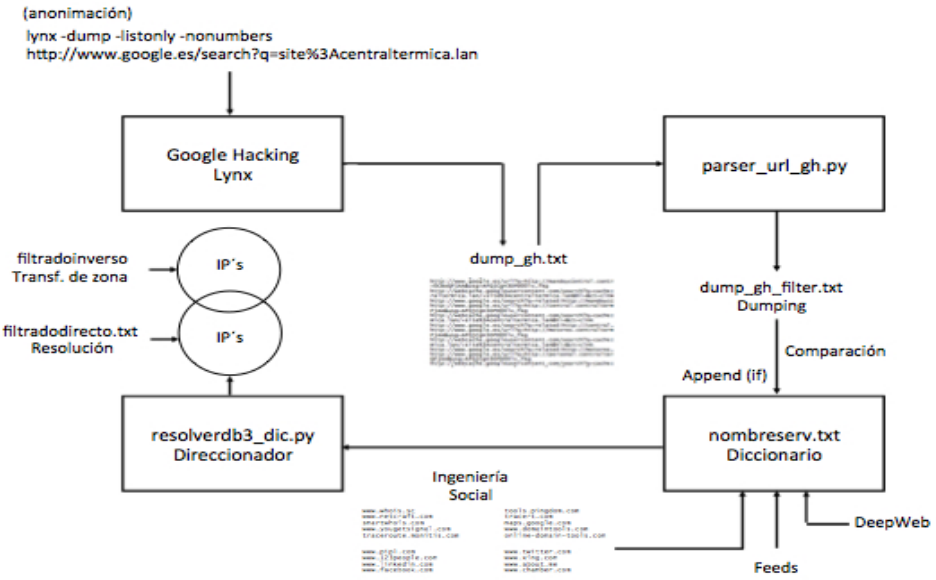
*Nota: Establezca el Diccionario (nombreserv.txt), Receptor (dump_gh.txt), el Filter (*dump_gh_filter.txt*) y Parser (parser_url_gh.py) en el mismo directorio de trabajo por simplicidad.*

Recuerde.., divida todo lo que pueda ya que en la simplicidad está el secreto tanto en el lenguaje utilizado (Python, Bash..), la codificación (cuanto más sencillo y claro mejor ya que volverá al código en numerosísimas ocasiones) y división modular en múltiples archivos o piezas de código independientes que le permitirá desarrollar y controlar aplicaciones más complejas o simplemente establecer tareas de automatización más eficientes aprovechando la potencia de Unix/GNU Linux.

parser_url_gh.py

```
#!/usr/bin/env python
# -*- coding: latin-1 -*-
#Versión:Python 2.7.6
#Check 24/05/2014
#Sistema:Backtrack5_release_10.04
#Kernel:linux 2.6.38
#Puede copiar,modificar y publicar este código en el medio que desee
#haciendo referencia de origen al autor del mismo.
#Utilice el mismo con responsabilidad en entornos seguros y controlables
#Tipo: parser

import os,sys,commands

def parser():
    dumper = open('dump_gh.txt','r')
    filtrado = open('dump_gh_filter.txt','w+')
    references = dumper.readlines()

    for dato_gh in references[:-1]:
        puntero = "related:http://"

        if ( dato_gh.find(puntero) != -1 ):
            inicio = dato_gh.find(puntero)
            final = dato_gh.find(dominio)
            host = dato_gh[inicio+15:final]
            filtrado.write(host + "\n")
    dumper.close()
    filtrado.close()
    return

def comparador():
    diccionario = open('nombreserv.txt','a+')
    dumperfiltrado = open('dump_gh_filter.txt','r')
    maquinasdiccionario = diccionario.readlines()
    maquinasdumperfiltrado = dumperfiltrado.readlines()
    listahostdiccionario = []

    for hostdiccionario in maquinasdiccionario:
        listahostdiccionario.append(hostdiccionario)

    listahostfiltrados = []
    for hostfiltrado in maquinasdumperfiltrado:
        listahostfiltrados.append(hostfiltrado)

    for host in listahostfiltrados:

        if host not in listahostdiccionario:
            listahostdiccionario.append(host)
            diccionario.write(host)
```

```
    diccionario.close()
    dumperfiltrado.close()
    return

print ""
print ("Versión: Free")
print ("Check 07/04/2014")
print ("Dumping.....")
print ""

if len(sys.argv) >= 2:
  dominio = "." + sys.argv[1]
  parser();
  comparador();
else:
  print "Error: especificar el dominio como argumento de referncia (References)"
  print ""
```



esquema de resolución

(*)Referencias

Autor: José Luis Prado Seoane
Freelance especializado en Seguridad Informática y Electrónica de sistemas y/o dispositivos en los entornos empresariales.
Blog: joseluispradoseoane.wordpress.com

(*)Comunidad

Compartir parte de tu trabajo y tiempo con la comunidad técnica (Researchers), sectores académicos, sectores profesionales de la seguridad, empresas del sector o con todos aquellos interesados en este mundo, etc.-, hace que el Hacking Ético bien enfocado adquiera su verdadero significado o sentido aportando un nuevo valor añadido a la seguridad en los entornos empresariales.

ADVERTENCIA

“ Actúe siempre con responsabilidad y recuerde, la finalidad es siempre el aprendizaje y la adquisición de conocimientos para la protección de los entornos informáticos en el ámbito de la empresa o la Ciberseguridad“

joseluispradoseoane.wordpress.com