PaperLab

Hacking Ético

Seguridad Informática

"automators"

automators (I)(II) GH/SH ++

Ciberseguridad

Revisión 9 -11.11

José luis Prado Seoane

automators_Labs , se presenta como un estudio técnico base explicativo y libre para la "*comunidad" de un proyecto más amplio en desarrollo que en la actualidad cuenta con más de treinta subprocesos relacionables locales o remotos basado en la búsqueda o recopilación, filtrado y sintetización de información pública a través de Internet formando parte del libro de Seguridad Informática y Hacking Ético, Hacking++, poniendo hincapié en uno de los cientos de Flags (parámetros) disponibles de exposición publica, para ello, se han utilizando en este Paper diferentes Tools en modo consola, así como recolectores públicos de captación tales como Google o Shodan por ser los más conocidos.

"automators_Labs" incluye el Paper publicado en los diferentes canales públicos de información técnica (paper.elautomator.pdf), y el nuevo proceso GH/SH (paper.elautomator2.pdf)

(paper.elautomator.pdf)

A través de este 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  y 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
```

nombreserv.txt

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

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

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	inurl:"MultiCameraFrame?Mode=Motion"

	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	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&ba=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 2**): 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 3**): 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%3Acentraltermi
ca.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%3Acentralt
ermica.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%3Acentralte
rmica.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%3Acentralterm
ica.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=0CCA
QFjAG&usg=AFQjCNETLm1YOKHWbRcDZjN_0NjwRHyCXQ
http://webcache.googleusercontent.com/search?q=cache:swsRDyDtTJQJ:http://comunicaciones.centraltermica.lan/wifi/+site%3A
centraltermica.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=AFQjCgH3
OPD00lv_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://mandoycontrol.centraltermica.lan/+site%3Acentralte
rmica.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=AFQjCgH3OPD00l
v_fkg
http://webcache.googleusercontent.com/search?q=cache:VRAkpgNsJ:http://central.centraltermica.lan/+site%3Acentraltermica.la
n&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=AFQjCgH3OPD00l
v_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.

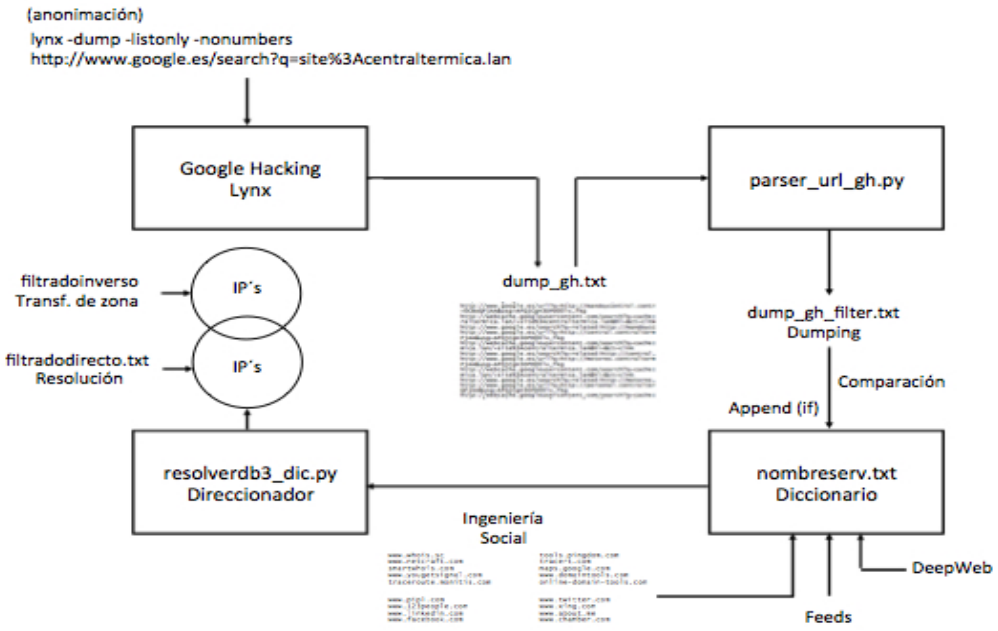
*Nota: Establezca el Diccionario (nombreserv.txt), Receptor (dump_gh.txt), el Filter (*dump_gh_filter.txt*) y Parser (parser_url_gh.py) en el mismo directorio de trabajo por simplicidad.*

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

(paper.elautomator2.pdf)

Si su ámbito de actuación es la Ciberseguridad o Ciberdefensa la recopilación de información, detección de vulnerabilidades y demás agentes implicados en la seguridad de infraestructuras críticas o de alta disponibilidad no deberán tomarse a la ligera. Imagínese que como analista de seguridad en la red (Ciberdefensa) se le asigna la monitorización de una Infraestructura crítica o dependencia estatal con exposición a Internet a modo de prevención, que permita alertar a sus superiores dentro de un procedimiento preestablecido de actuación para que se tomen las actuaciones técnicas, de aviso e incluso de iniciación jurídica enmarcadas dentro de la normativa en nuestro caso Europea de retirada de indexaciones o historiales de los navegadores públicos como Google, Bing, entre otros, en cumplimiento de las sentencias al respecto ("el derecho a olvidar"), que evite que terceros con malas intenciones puedan utilizar las mismas para iniciar o conformar un ataque dirigido, sabía que un navegador puede indexar realizando su cometido una URL con un Exploit asociado específico o simplemente una página en la que su código linkea todo tipo de Exploits previamente seleccionados desencadenado el ataque por usted preservando de esta forma su "anonimato" y lo peor aún, que dicha acción permanecerá indexada y en comunidad para terceros y ya sabe, tomo tiene un precio. Imagínese esta información en manos de un atacante por simplificar la cuestión. Si logra determinar y actuar en consecuencia con rapidez y profesionalidad estará contribuyendo a la seguridad y protección de lo que le ha sido encomendado.

Continuando con la recopilación a través de fuentes públicas disponibles en la red realizaremos un estudio del denominado Google para Hackers el conocido Shodan (www.shodanhq.com), por cierto, no olvide que existen en Internet otros proyectos similares de gran interés. A diferencia de la utilización de Google como fuente para la recopilación de información pública, Shodan no recupera u obtiene contenidos, su tecnología le permitirá buscar computadoras y dispositivos en la Red por el software utilizado en los servicios que estos publican o exponen en

la Red asociado a los puertos 21,22,25,80,143,110 23 y 443 (estos dos últimos necesitará un add-on). Shodan nos devuelve estas cabeceras HTTP y Banners asociados a los servicios (HTTP, FTP, SSH, SNMP, SIP..) aún así, establece limitaciones a las búsquedas, filtros o modificadores avanzados, en primer lugar por paginación (<1) en sus búsquedas (sólo le mostrará 10 resultados) por lo que deberá registrase para obtener más resultados y capacidades ampliando los resultados retornados a cien (100), en segundo lugar en su API que aunque se haya registrado y aumente como hemos comentado el rango de búsquedas retornadas (100) establece más restricciones en los modificadores de búsquedas como City, Country, etc.-, por lo que si necesitara por su trabajo ampliar "funcionalidades", deberá adherirse al plan de pago suministrado por la plataforma en sus diferentes modalidades de "Queries", que en la actualidad se comercializan a través de diferentes planes de desarrollo (https://developer.shodan.io/).

En relación al procedimiento que utilizaremos para la recuperación de la información de Shodan, disponemos de varias formas potenciales, la primera es la utilización del API correspondiente suministrado por la plataforma con sus limitaciones de una forma directa (GET) a través de su navegador Web de trabajo (TOR) que le devolverá un Htm(l) que deberá volcar a su disco de trabajo y posteriormente realizar un Parser específico para el análisis, filtrado y síntesis de la información, la segunda es codificar su propio Script(s) (Python, Ruby, NodeJs) utilizando su API y realizando nuevamente un Parser específico como hemos comentado (parser_API_sh.py) o simplemente utilizando como hemos realizado en el Lab anterior a Lynx como herramienta de trabajo de una forma directa (References) o en modo GET(API), el cuál recordemos, nos "dumpeará" la salida hacia un file (dump_sh.txt) que nos permitirá determinar y filtrar los datos a través de Scripts desarrollados para tal fin que en nuestro caso serán; un Parser (parser_url_sh.py) con volcado (dump_sh_filter.txt) hacia el diccionario común (nombreserv.txt) y direccionado hacia el Resolver (resolverdb3_dic.py). Estas tres opciones son perfectamente válidas y más aún, complementarias, por lo que declinarse por una u otra o el trabajo en conjunto de las tres técnicas, estará en función de sus necesidades. El uso de las API´s asociadas a las plataformas públicas como Google, Bing y en este caso Shodan tienen el inconveniente de que quedará registrada su actividad (Remember), y aunque le digan que no, hágame caso, sucederá y su identidad será relacionada. Todo esto un atacante especializado lo sabe, para ello tomará en caso de ser necesaria su implementación las precauciones necesarias en lo que a su identidad y datos suministrados se refiere y anonimación correspondiente, en su caso, y en función de su trabajo o desempeño de seguridad, deberá hacer lo mismo, ya sabe, si se dedica a la Ciberseguridad o la Ciberdefensa deberá garantizar su identidad frente a terceros en sus investigaciones. Shodan pone a disposición tres tipos de API´s; REST API, STREAMMING API y EXPLOITS API. Para la recopilación de información con paginación (>1) y el uso de la API, necesitará registrarse a través de "Shodan Account" (https://account.shodan.io/login) para disponer de su {API_KEY}, que deberá guardar cuidadosamente por seguridad. Le recomiendo que para su trabajo almacene la misma en un archivo de texto en una unidad externa o servidor específico protegido de claves.

A continuación utilizaremos la técnica de "References" tal y como hemos hecho en Google que le permitirá dumpear la salida al fichero en disco (dump_sh.txt)

```
root@lab:/libro/modulo1#
lynx -listonly -nonumbers -dump http://www.shodanhq.com/search?q=hostname%3Acentraltermica.lan > dump_sh.txt
```

dump_sh.txt (búsqueda References)

(Se han dumpeado de Lynx varias resoluciones de Shodan)

```
References

...

http://192.168.1.225/
http://www.shodanhq.com/search?q=hostname%3Acentraltermica.lan+city%3A%22Madrid%22
http://accesos.centraltermica.lan/
http://129.168.1.234/
http://www.shodanhq.com/search?q=hostname%3Acentraltermica.lan+city%3A%22Madrid%22
http://alarmas.centraltermica.lan/
http://129.168.1.239/
http://www.shodanhq.com/search?q=hostname%3Acentraltermica.lan+city%3A%22Madrid%22
http://mandoycontrol.centraltermica.lan/
http://129.168.1.231/
http://www.shodanhq.com/search?q=hostname%3Acentraltermica.lan+city%3A%22Zaragoza%22
http://nodo2.centraltermica.lan/
http://ns1.centraltermica.lan/

...
```

(**Practica 4**): Reutilice y codifique el Parser anterior (parser_url_gh.py)-->(parser_url_sh.py) con volcado (dump_sh_filter.txt) hacia el diccionario común (nombreserv.txt). Siempre puede re-codificar el Parser anterior e

integrar las dos opciones, pero le recuerdo nuevamente que la simplicidad y la división de procesos garantizará entre otras cosas su reutilización o actualización en futuros cambios.

A continuación le mostraré uno de los métodos "GET" + {API_KEY} disponibles como ejemplo en una búsqueda, de los múltiples existentes que le aconsejo que practique o experimente con ellos, que podrá automatizar a través de Lynx u otro navegador de consola, dumpearlo a un archivo en disco y sintetizarlo a través de un Script que le de la forma que verá más abajo en el ejemplo o simplemente si lo desea, hacerlo de una forma manual a un archivo en disco (html_sh.txt) a través de su navegador Web (TOR) el cuál, le devolverá como hemos comentado un Htm(l) finalizando codificando un Parser específico (parser_API_sh.py) para el análisis, filtrado y síntesis de la información en función de lo que esté buscando.

(**Practica 5**): Automatice el proceso anterior a través de un Script en Python para la sintetización del GET

https://api.shodan.io/shodan/host/search?key={YOUR_API_KEY}&query={query}&facets={facets}
(Busca el la base de Datos de Shodan información (Banners) asociado al Query proporcionado)

https://api.shodan.io/shodan/host/search?key={xxxxxxxxxx....}&query={centraltermica.lan}

html_sh.txt (búsqueda GET)
(Se han dumpeado el GET HTM(L) de Shodan)

{"matches":
[
{
"info": "(Win32) OpenSSL/0.9.8y PHP/5.4.16",
"product": "Apache httpd",
"hostnames": ["nodo2.centraltermica.lan"],
"version": "2.4.4",
"timestamp": "2013-05-26T19:19:12.4222",
"isp": "xxxxxxx de Espana",
"cpe": "a:apache:http_server:2.4.4",
"data": "HTTP/1.0 302 Found\r\nDate: Mon, 26 May 2013 19:18:48 GMT\r\nServer: Apache/2.4.4 (Win32) OpenSSL/0.9.8y PHP/5.4.16\r\nX-Powered-By: PHP/5.4.16\r\nLocation: http://centraltermica.lan\r\nContent-Length: 0\r\nContent-Type: text/html\r\n\r\n",
"port": 80,
"location": {"city": "Madrid", "region_name": null, "area_code": null, "longitude": -x.xxxxxx, "country_code3": "ESP", "latitude": xx.xxxx, "postal_code": "xxxxx", "dma_code": null, "country_code": "ES", "country_name": "Spain"},
"ip": xxxxxxxxxxx,
"domains": ["xxxxxxxxxx.com"],
"org": " xxxxxxx de Espana",
"os": null,
"asn": "Axxxxx",
"ip_str": "192.168.1.231"
},

{
"product": "nginx",
"title": "301 Moved Permanently",
"timestamp": "2013-05-21T22:14:57.92..",
"isp": "xxxISPxx",
"cpe": "a:xxxxxxxx:nginx",
"data": "HTTP/1.0 301 Moved Permanently\r\nServer: nginx\r\nDate: Wed, 21 May 2013 22:13:17 GMT\r\nContent-Type: text/html\r\nContent-Length: 178\r\nConnection: keep-alive\r\nLocation: http://centraltermica.lan\r\n\r\n",
"port": 80,
"location": {"city": null, "region_name": null, "area_code": null, "longitude": -x.0, "country_code3": "ESP", "latitude": xx.0, "postal_code": null, "dma_code": null, "country_code": "ES", "country_name": "Spain"},
"ip": xxxxxxxxxxx,
"domains": ["ono.com"],
"org": " xxxISPxx",
"os": null,
"asn": "Axxxxx",
"hostnames": ["fire.centraltermica.lan"],
"ip_str": "192.168.1.223"
},

{
"info": "(Ubuntu)",
"product": "Apache httpd",
"os": null,
"timestamp": "2013-05-26T19:19:12.4222",
"isp": "xxxxxxxxx B.V.",
"cpe": "a:apache:http_server:2.2.2",
"asn": "Axxxxxx",

"version": "2.2.22",
"location": {"city": "Madrid", "region_name": null, "area_code": null, "longitude": x.xxxxxxxxx, "country_code3": "ESP", "country_name": "Spain", "postal_code": null, "dma_code": null, "country_code": "ES", "latitude": xx.xxxxx...},
"ip": xxxxxxxxxx,
"domains": ["xxxxxxxxx.com"],
"org": "xxxxxxxxxxx",
"data": "HTTP/1.0 302 Found\r\nDate: Tue, 06 May 2013 04:30:16 GMT\r\nServer: Apache/2.2.22 (Ubuntu)\r\nX-Powered-By: PHP/5.3.10-1ubuntu3.9\r\nLocation: http://centraltermica.lan\r\nVary: Accept-Encoding\r\nContent-Length: 4\r\nContent-Type: text/html\r\n\r\n",
"port": 80,
"hostnames": ["video.centraltermica.lan"],
"ip_str": "192.168.1.224"
},

{
"info": "(Win32) OpenSSL/0.9.8y PHP/5.4.16",
"product": "Apache httpd",
"os": null,
"timestamp": "2013-05-05T06:11:08.xxxxxx",
"isp": "xxxxxxx de Espana",
"cpe": "a:apache:http_server:2.4.4",
"asn": "Axxxxx",
"version": "2.4.4",
"location": {"city": "Madrid", "region_name": null, "area_code": null, "longitude": -x.xxxxxxxxxxxxx, "country_code3": "ESP", "country_name": "Spain", "postal_code": null, "dma_code": null, "country_code": "ES", "latitude": xx.xxxxxxxxxxxxx},
"ip": xxxxxxxxxx,
"domains": ["xxxxxxxx.net"],
"org": "xxxxxxxxx de Espana",
"data": "HTTP/1.0 302 Found\r\nDate: Mon, 05 May 2013 06:12:07 GMT\r\nServer: Apache/2.4.4 (Win32) OpenSSL/0.9.8y PHP/5.4.16\r\nX-Powered-By: PHP/5.4.16\r\nLocation: http://centraltermica.lan\r\nContent-Length: 0\r\nContent-Type: text/html\r\n\r\n",
"port": 80,
"hostnames": ["suministro.centraltermica.lan"],
"ip_str": "192.168.1.230"
},

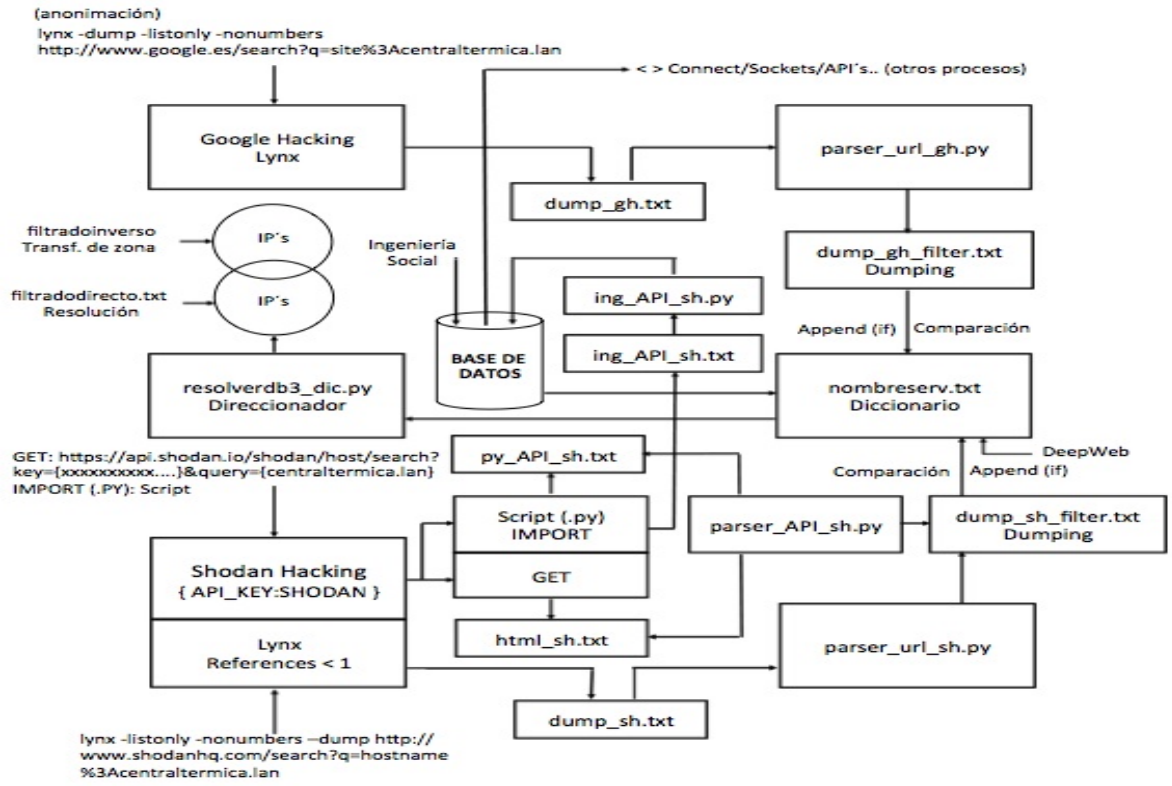
{
"info": "(Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_xxxxx PHP/5.3.1 mod_apreq2-xxxxxxxx/2.7.1 mod_perl/2.0.4 Perl/v5.10.1",
"product": "Apache httpd",
"os": null,
"timestamp": "2013-05-04T15:14:06.xxxxxx",
"isp": "xxxxxxxxxx de Espana",
"cpe": "a:apache:http_server:2.2.14",
"asn": "Axxxxx",
"version": "2.2.14",
"location": {"city": null, "region_name": null, "area_code": null, "longitude": -x.0, "country_code3": "ESP", "country_name": "Spain", "postal_code": null, "dma_code": null, "country_code": "ES", "latitude": xx.0},
"ip": xxxxxxxxxx,
"domains": ["xxxxxxxx.net"],
"org": "xxxxxxxxxx de Espana",
"data": "HTTP/1.0 302 Found\r\nDate: Sun, 04 May 2013 15:14:xx GMT\r\nServer: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_xxxxx PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1\r\nX-Powered-By: PHP/5.3.1\r\nLocation: http://centraltermica.lan\r\nContent-Length: 0\r\nContent-Type: text/html\r\n\r\n",
"port": 80,
"hostnames": ["perimetros.centraltermica.lan"],
"ip_str": "192.168.1.235"
},

{
"product": "LiteSpeed httpd",
"os": null,
"title": " 302 Found\r\n",
"timestamp": "2013-05-03T18:28:56.xxxxxx",
"isp": "xxxxxxxxx SL",
"asn": "Axxxxxx",
"hostnames": ["mail1.centraltermica.lan"],
"location": {"city": null, "region_name": null, "area_code": null, "longitude": xx.0, "country_code3": "ESP", "country_name": "Spain", "postal_code": null, "dma_code": null, "country_code": "ES", "latitude": xx.0},
"ip": xxxxxxxxxx,
"domains": ["xxxxxxxx.com"],
"org": "xxxxxxx SL",
"data": "HTTP/1.0 302 Found\r\nDate: Sat, 03 May 2013 18:29:xx GMT\r\nServer: LiteSpeed\r\nConnection: Keep-Alive\r\nKeep-Alive: timeout=5, max=100\r\nCache-Control: no-cache, no-store, must-revalidate, max-age=0\r\nLocation: http://centraltermica.lan/\r\nVary: User-Agent\r\nContent-Type: text/html\r\nContent-Length: 2199\r\n\r\n",
"port": 80,

"ip_str": "192.168.1.106"
},

{
"info": "(Win64) mod_ssl/2.2.22 OpenSSL/1.0.0g PHP/5.3.13",
"product": "Apache httpd",
"os": "Windows 7 or 8",
"title": "xxxxxxxxxxxx título",
"timestamp": "2013-02-23T00:28:25.xxxxxx",
"isp": "xxxxxxxxxx S.L.",
"uptime": 11xxx,
"cpe": "a:apache:http_server:2.2.22",
"ip": xxxxxxxxxx,
"version": "2.2.22",
"link": "Ethernet or modem",
"location": {"city": null, "region_name": null, "area_code": null, "longitude": -x.0, "country_code3": "ESP", "country_name": "Spain", "postal_code": null, "dma_code": null, "country_code": "ES", "latitude": xx.0},
"asn": "Axxxxxx",
"domains": ["xxxxxxxxxx.com"],
"org": "xxxxxxxxxx S.L.",
"data": "HTTP/1.0 302 Found\r\nDate: Sun, 23 Feb 2013 00:31:xx GMT\r\nServer: Apache/2.2.22 (Win64) mod_ssl/2.2.22 OpenSSL/1.0.0g PHP/5.3.13\r\nX-Powered-By: PHP/5.3.13\r\nLocation: http://centraltermica.lan\r\nContent-Length: 7xx\r\nContent-Type: text/html\r\n\r\n",
"port": 80
}
],
"total": 6}

A continuación le muestro el esquema de procesos (1 de 36)) ampliado así como, los prototipos de "Queries" (GET); REST API, STREAMING API y EXPLOITS API que tiene disponibles en la actualidad, y que podrá documentarse a mayores en opciones y parámetros a través del siguiente enlace (https://developer.shodan.io/api), y recuerde, si automatiza la tarea a través de un Script(s) aumentará su capacidad de recopilación de información. El campo de aplicación es inmenso, imagínese que desarrolla diferentes modelos de captación de datos (esquemas de procesos), - *que en nuestros ejemplos se focalizo en "Hostnames" asociados a un dominio dado* -, a través de procesos paralelos que combinados permitan sintetizar y filtrar la información hacia un objetivo en concreto y además, imagínese que alimentan o realimentan en parte o en su totalidad de los datos obtenidos en las consultas a diferentes procesos de Ingeniería Social automáticos (Scripts) fuera de los modelos tradicionales existentes. Se sorprenderá de la potencia de esta técnica y eso sí , vaya pensando en aumentar la capacidad de sus sistemas de Backup, ya que la información recibida será totalmente exponencial y difícil de cuantificar en tamaño por no decir, otros aspectos relacionados con el procesamiento y soporte informático que deberá tener en cuenta.



- V(2) esquema de resolución Google & Shodan Hacking -

REST API:
https://api.shodan.io/shodan/host/{ip}?key={YOUR_API_KEY}
https://api.shodan.io/shodan/host/count?key={YOUR_API_KEY}&query={query}&facets={facets}
https://api.shodan.io/shodan/host/search?key={YOUR_API_KEY}&query={query}&facets={facets}

https://api.shodan.io/shodan/host/search/tokens?key={YOUR_API_KEY}&query={query}
https://api.shodan.io/shodan/services?key={YOUR_API_KEY}
https://api.shodan.io/dns/resolve?hostnames={hostnames}&key={YOUR_API_KEY}
https://api.shodan.io/dns/reverse?ips={ips}&key={YOUR_API_KEY}
https://api.shodan.io/tools/myip?key={YOUR_API_KEY}
https://api.shodan.io/api-info?key={YOUR_API_KEY}

REST STREAMING:
https://stream.shodan.io/shodan/banners?key={YOUR_API_KEY}
https://stream.shodan.io/shodan/geo?key={YOUR_API_KEY}
https://stream.shodan.io/shodan/ports/1434,27017,6379?key={YOUR_API_KEY}

EXPLOITS API:
https://exploits.shodan.io/api/search?query={query}&key={YOUR_API_KEY}
https://exploits.shodan.io/api/count?query={query}&key={YOUR_API_KEY}

A continuación instalaremos las librerías se Shodan y desarrollaremos un sencillo Script "IMPORT" en Python (.py) que utilice el API de Shodan que denominaremos (import_API.py), el cuál, volcará la información hacia el fichero (py_API_sh.txt) recolector de datos y alimentará el recolector de datos DB (ing_API_sh.txt) con información puntual y específica relacionada como por ejemplo.-, datos de Geolocalización (Lon/Lat) que podrán ser utilizados por otros procesos locales o remotos API como Google Maps, entre otros, en el desarrollo de procesos de recopilación y localización. Finalizaremos desarrollando el Parser (parser_API_sh.py)-->(dump_sh_filter.txt) que analice el par de ficheros de datos (html_sh.txt : py_API_sh.txt) que utilizará según las necesidades puntuales de su trabajo sea de una forma manual o automatizando este tipo de análisis uniéndolo con otros procesos de captación de información.

root@lab:/# apt-get update

root@lab:/# apt-get install python-setuptools

root@lab:/# easy_install shodan (easy_install -U shodan---> para actualizaciones)

Searching for shodan
Reading http://pypi.python.org/simple/shodan/
Best match: shodan 1.0.3
Downloading https://pypi.python.org/packages/source/s/shodan/shodan-1.0.3.tar.gz#md5=hjb87098jh.....
Processing shodan-1.0.3.tar.gz
Running shodan-.....

import_API.py

(python import_API.py <dominio>)

```
#!/usr/bin/env python
# -*- coding: latin-1 -*-
#Versión:Python 2.6.5
#Check 13/05/2014
#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: IMPORT

import os,sys,commands
from shodan import WebAPI
APIKEY = "<copie aquí su APIKEY>"
sh=WebAPI(APIKEY)

def feed_dic():
```

```
  print "Obteniendo Hostnames ... [] "
  try:
    dumper = open('py_API_sh.txt','w+')
    resultados = sh.search(busqueda)

    for i in resultados['matches']:
      host = '\n'.join(i['hostnames']) + '\n'

      if ( len(host) != 1 ):
        dumper.write(host)
    dumper.close()

  except Exception, e:
    print "Error: %s" % e
  return


def basededatos():
  print "Obteniendo Datos _DB ... [] "
  try:
    dumper = open('ing_API_sh.txt','w+')
    resultados = sh.search(busqueda)

    for i in resultados['matches']:
      host = "Host:%s" % '\n'.join(i['hostnames']) + '\n'
      ip = "Ip:%s" % ''.join(i['ip']) + '\n'
      so = "So:%s" % str(i['os']) + '\n'
      puerto = "Puerto:%s" % str(i['port']) + '\n'
      pais = "Pais:%s" % str(i['country_name']) + '\n'
      ciudad = "Ciudad:%s" % str(i['city']) + '\n'
      latitud = "Lat:%s" % str(i['latitude']) + '\n'
      longuitud = "Lon:%s" % str(i['longitude']) + '\n'

      if ( len(host) != 1 ):
        dumper.write(host)
        dumper.write(ip)
        dumper.write(so)
        dumper.write(puerto)
        dumper.write(pais)
        dumper.write(ciudad)
        dumper.write(latitud)
        dumper.write(longuitud)
        dumper.write('-----' * 10 + '\n')
    dumper.close()

  except Exception, e:
    print "Error: %s" % e

  return

print ""
print ("Versión: Free")
print ("Check 14/06/2014")
print ("Dumping.....")
print ""

if len(sys.argv) >= 2:
busqueda = "hostname:" + sys.argv[1]
feed_dic();
basededatos();
else:
print "Error: especificar el dominio de análisis"
print ""
```

parser_API_sh.py

(Se han dumpeado el API/GET HTM(L) de Shodan
al Dumper (filtro) y diccionario)

(python parser_API_sh.py <dominio>)

```
#!/usr/bin/env python
# -*- coding: latin-1 -*-

#Versión:Python 2.6.5
#Check 10/06/2014
```

```
#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
#Tipo: parser_shodan

import os,sys,commands

def parser_html():

  try:

    fuentehtml = open('html_sh.txt','r')
    filtradosh = open('dump_sh_filter.txt','w+')
    datoshtml = fuentehtml.readlines()

    for maquina in datoshtml:
      puntero = '"hostnames": ["'
      puntero2 = '"],'

      if ( maquina.find(puntero) != -1 ):
        inicio = maquina.find(puntero)
        final = maquina.find(puntero2)
        hosthtml = maquina[inicio+15:final]
        filtradosh.write(hosthtml + "\n")

    fuentehtml.close()
    filtradosh.close()

  except Exception, e:
    print "Error: %s" % e

  return

def parser_py():

  try:

    fuenteapi = open('py_API_sh.txt','r')
    filtradosh = open('dump_sh_filter.txt','a+')
    datosapi = fuenteapi.readlines()
    datossh = filtradosh.readlines()

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

    listahostapi = []
    for hostapi in datosapi:
      listahostapi.append(hostapi)

    for host in listahostapi:

      if host not in listahostfiltrados:
        listahostfiltrados.append(host)
        filtradosh.write(host)

    fuenteapi.close()
    filtradosh.close()

  except Exception, e:
    print "Error: %s" % e

  return

def comparador():

  try:

    diccionario = open('nombreserv.txt','a+')
    dumperfiltrado = open('dump_sh_filter.txt','r')
    maquinasdiccionario = diccionario.readlines()
    maquinasdumperfiltrado = dumperfiltrado.readlines()

    listahostdiccionario = []
```

```
    for hostdiccionario in maquinasdiccionario:
      print hostdiccionario[:-1]
      listahostdiccionario.append(hostdiccionario[:-1])

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

    for host in listahostfiltrados:
      print host[:-(len(dominio)+1)]

      if host[:-(len(dominio)+1)] not in listahostdiccionario:
        listahostdiccionario.append(host)
        diccionario.write(host[:-(len(dominio)+1)] + "\n")

    diccionario.close()
    dumperfiltrado.close()

  except Exception, e:
    print "Error: %s" % e

  return

print ""
print ("Versi√≥n: Free")
print ("Check 10/06/2014")
print ("Dumping.....")
print ""

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

(*)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.

Dominio estudio:

(*)Dominio utilizado para la realización de este PaperLab: centraltermica.lan
(el mismo es local/Ip´s y permite presentar el desarrollo del proceso de una forma ordenada y segura)

ADVERTENCIA

Sea consciente en todo momento que los conocimientos y herramientas presentadas si se emplean contra terceros con independencia del medio, tecnología, ubicación, ámbito, etc.-, sin su autorización expresa, pueden ser en algunos casos ilegales. El autor, no se hace responsable del uso indebido en cualquiera de sus formas, de los actos o irresponsabilidades que pudieran derivarse de la adquisición de dichos conocimientos, técnicas utilizadas, herramientas, etc.-, ante cualquier irresponsabilidad o ilegalidad que pudiera derivarse.

Tiene autorización para copiar y difundir dicho documento por el medio que desee y publicar partes del mismo siempre que haga referencia a su autor.

“ 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