

Rodrigo Castillo Camargo

Taller de Footprinting

1: Footprinting:

Toda actividad que nosotros hacemos, creamos o buscamos en internet deja una huella digital que es accesible para cualquier persona que tenga a disposición el internet.

El “Footprinting” hace referencia al regateo de información que se puede ejecutar a través de técnicas de búsqueda con el fin de encontrar información sensible de algún objetivo en específico, para fines del taller , haré Footprinting sobre la escuela colombiana de ingeniería julio garavito.

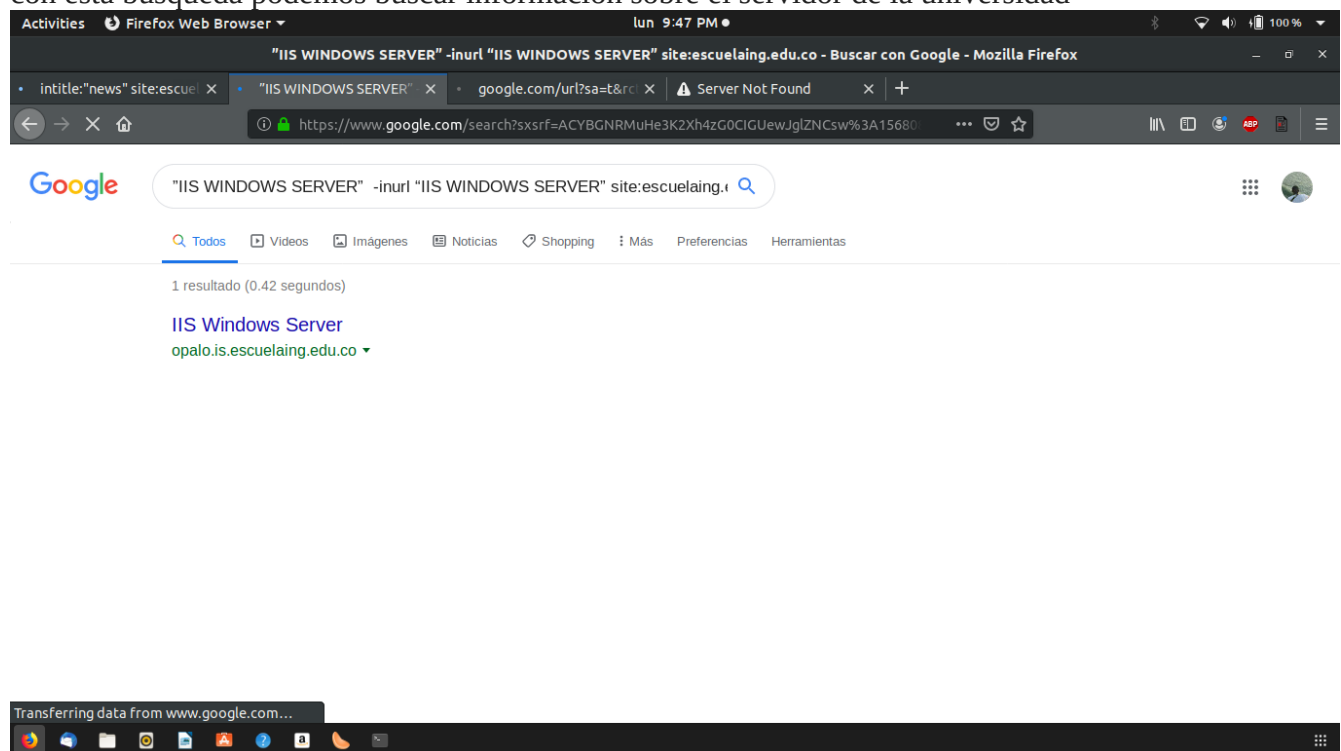
Parte 1- Búsquedas avanzadas en google

Primera búsqueda: `intitle:"news" site:escuelaing.edu.co`

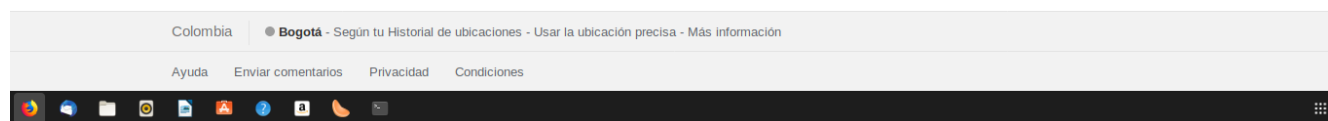
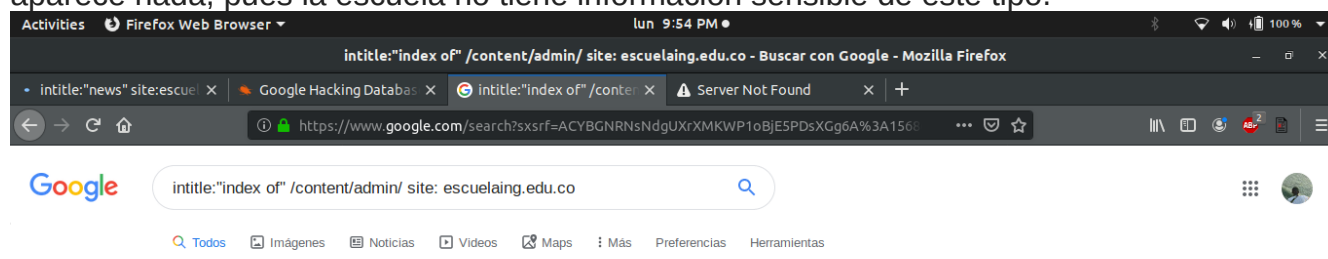
con ésta búsqueda, podemos buscar información sobre noticias del laboratorio de la escuela colombiana de ingeniería, acá nos podemos informar sobre los lugares a los que tienen acceso los estudiantes en el laboratorio, sobre los dispositivos que éste posee, sobre la información del laboratorio que poseen los estudiantes, sobre los estudiantes de ingeniería que tienen acceso a la sala de sistemas puesto que fueron posicionados como monitores de ésta...etc.

Segunda Búsqueda :`Intitle:"IIS WINDOWS SERVER" -inurl "IIS WINDOWS SERVER" site:escuelaing.edu.co`

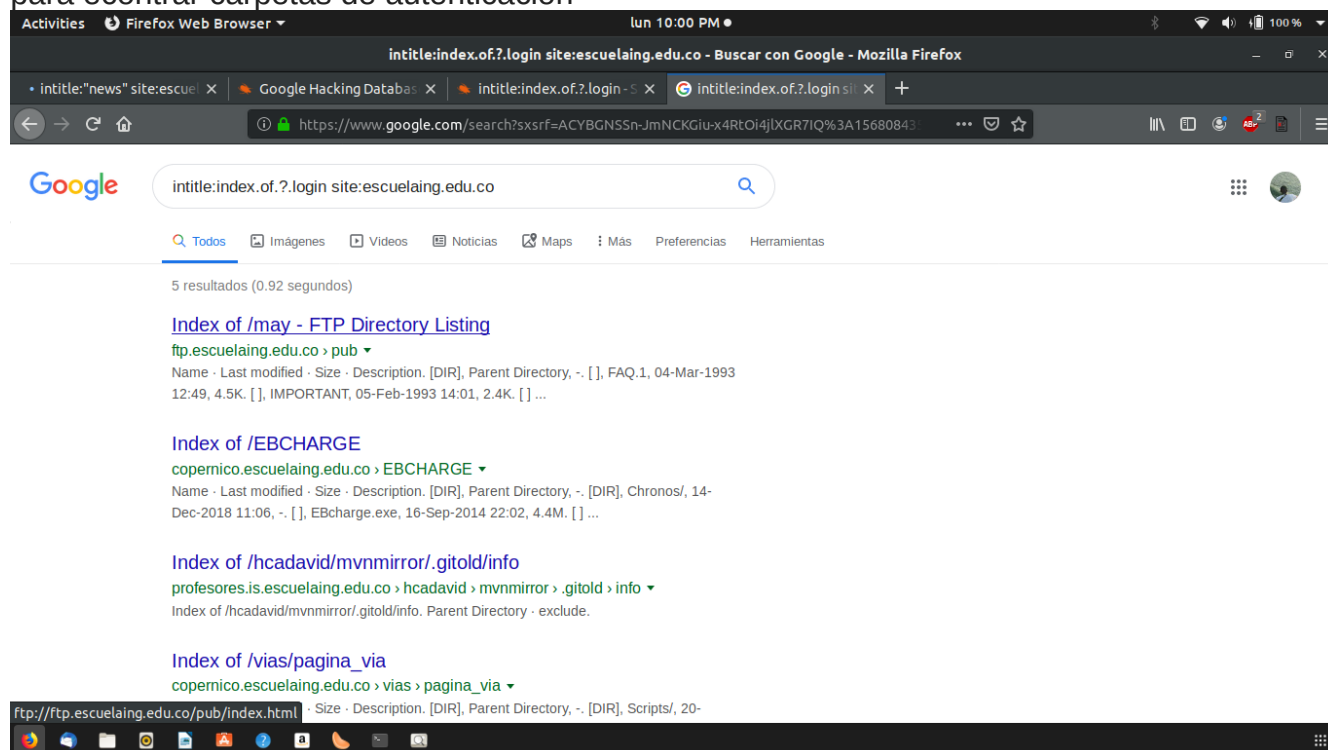
con esta búsqueda podemos buscar información sobre el servidor de la universidad

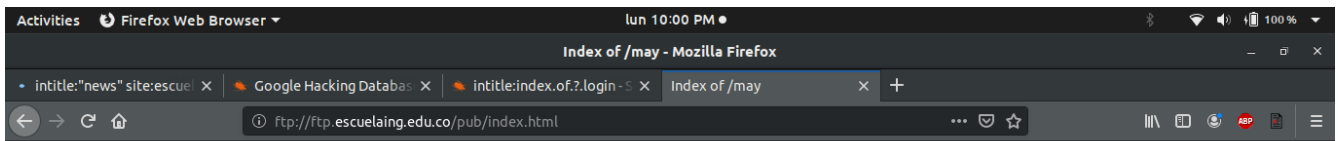


tercera búsqueda: [intitle:"index of" /content/admin/ site:escuelaing.edu.co](#)
por ejemplo, en esta búsqueda de directorios sensibles del contenido del administrador, no aparece nada, pues la escuela no tiene información sensible de este tipo.



Cuarta búsqueda: [intitle:index.of.?.login site:escuelaing.edu.co](#) es un comando que se usa para encontrar carpetas de autenticación



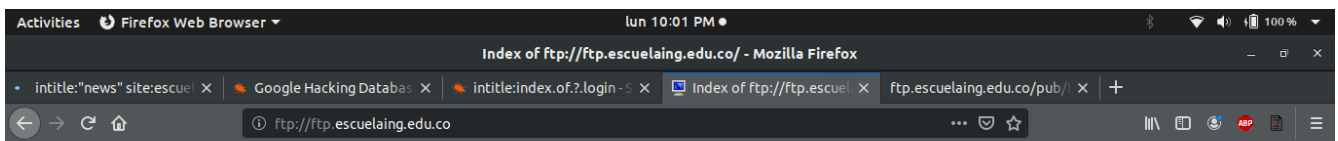


Index of /may

[ICO] [Name](#) [Last modified](#) [Size](#) [Description](#)

[DIR]	Parent Directory	-		
[]	FAQ.1	04-Mar-1993 12:49	4.5K	
[]	IMPORTANT	05-Feb-1993 14:01	2.4K	
[]	INTRO	11-Mar-1993 20:21	18K	
[]	REFERENCE	05-Mar-1993 20:18	24K	
[]	TBD	18-Jan-1993 21:10	765	
[]	USER-GUIDE	12-Mar-1993 16:23	19K	
[]	examples	07-Jan-1993 18:06	556	
[]	may-2.09.tar.gz	23-Mar-1997 14:27	83K	

Apache/2.2.14 (Ubuntu) Server at linas.org Port 80

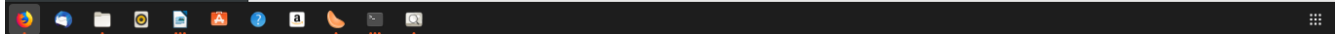


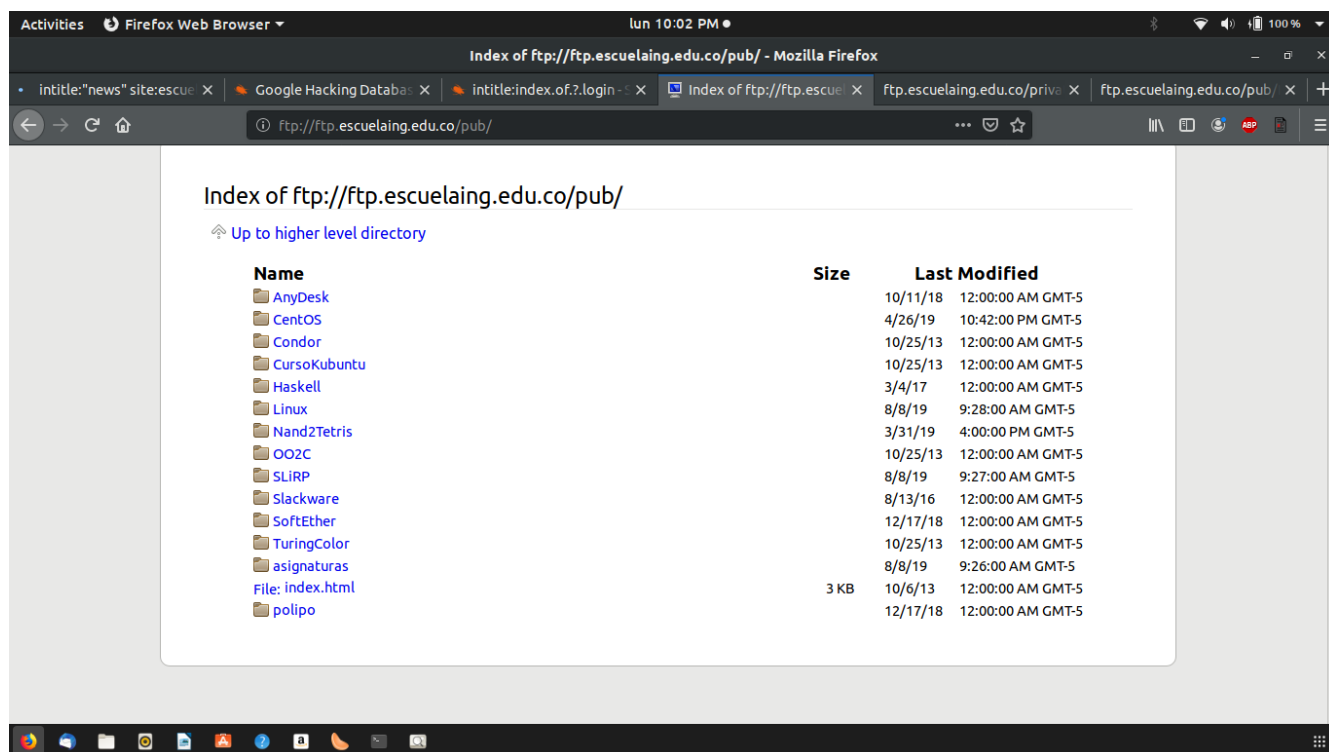
Index of ftp://ftp.escuelaing.edu.co/

[Up to higher level directory](#)

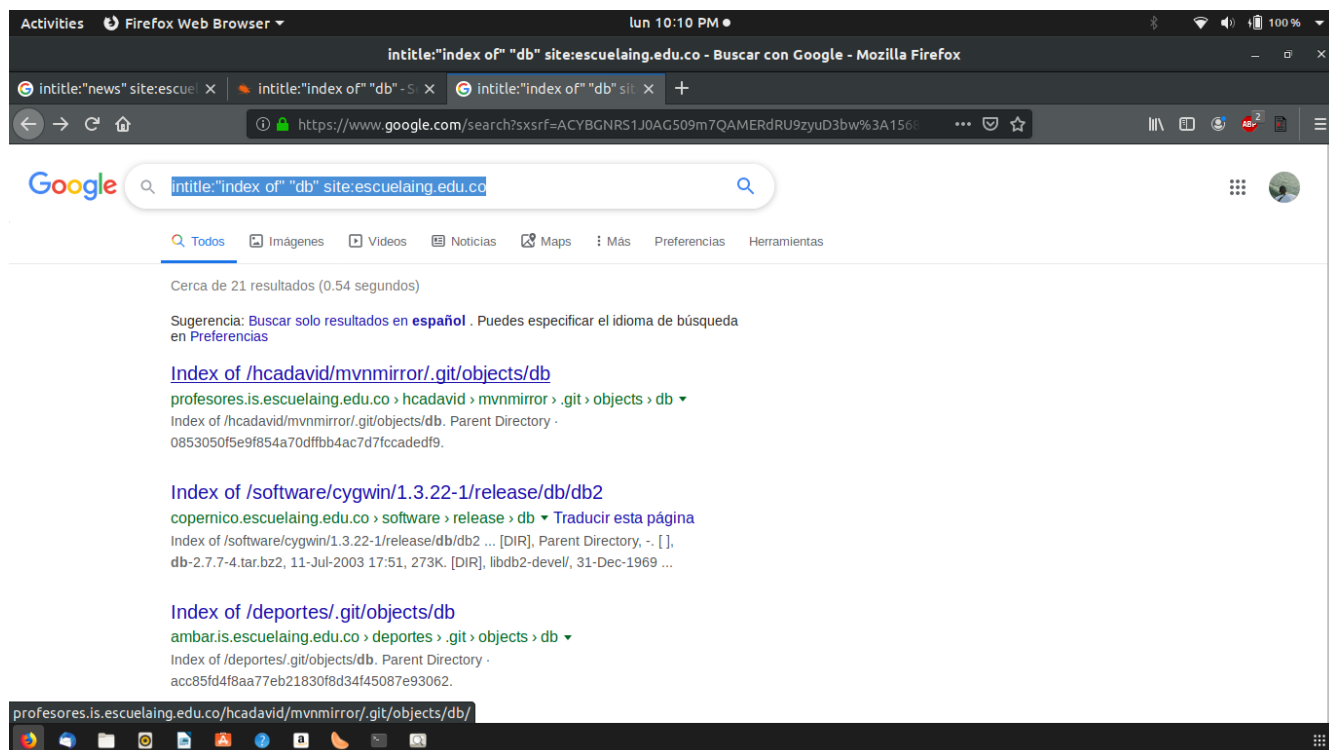
Name	Size	Last Modified
File: index.html	1 KB	2/4/14 12:00:00 AM GMT-5
Folder: private		7/17/19 3:52:00 PM GMT-5
Folder: pub		8/8/19 9:28:00 AM GMT-5

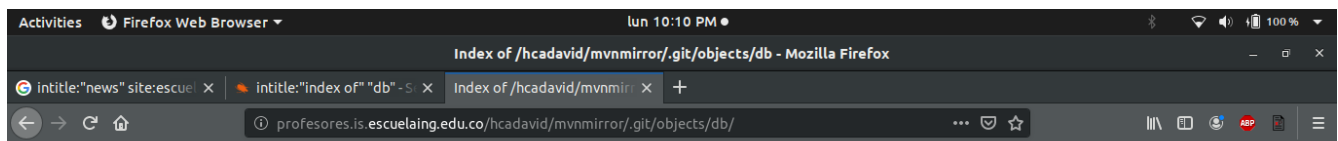
ftp://ftp.escuelaing.edu.co/private/





quinta busqueda: intitle:"index of" "db" site:escuelaing.edu.co
 esta busqueda permite encontrar directorios sensibles que usen la palabra "db" que quiere decir data bases, da acceso a información sobre los servidores de la escuela de ingenieros que puede ser usada para futuros ataques





Index of /hcadavid/mvnmirror/.git/objects/db

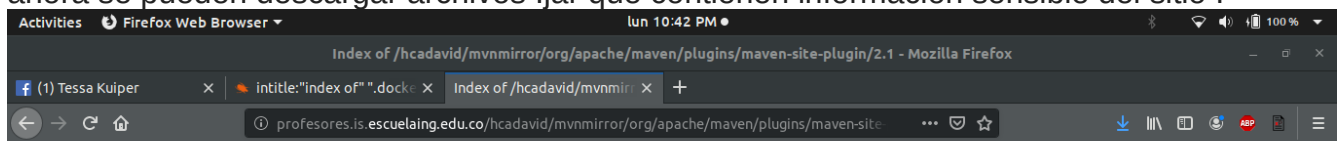
- [Parent Directory](#)
- [0853050f5e9f854a70dffbb4ac7d7fccadedf9](#)



con lo que tenemos acceso a bases de datos sensibles de los estudiantes y profesores de la universidad.

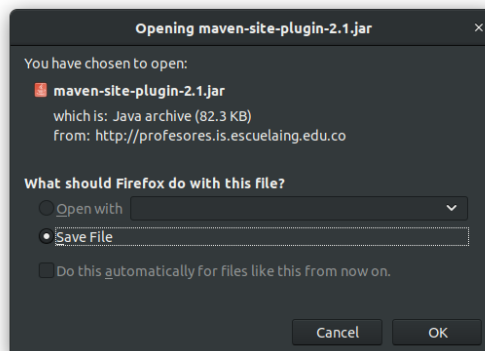
Sexta búsqueda: `intitle:"plugin" site :escuelaing.edu.co`

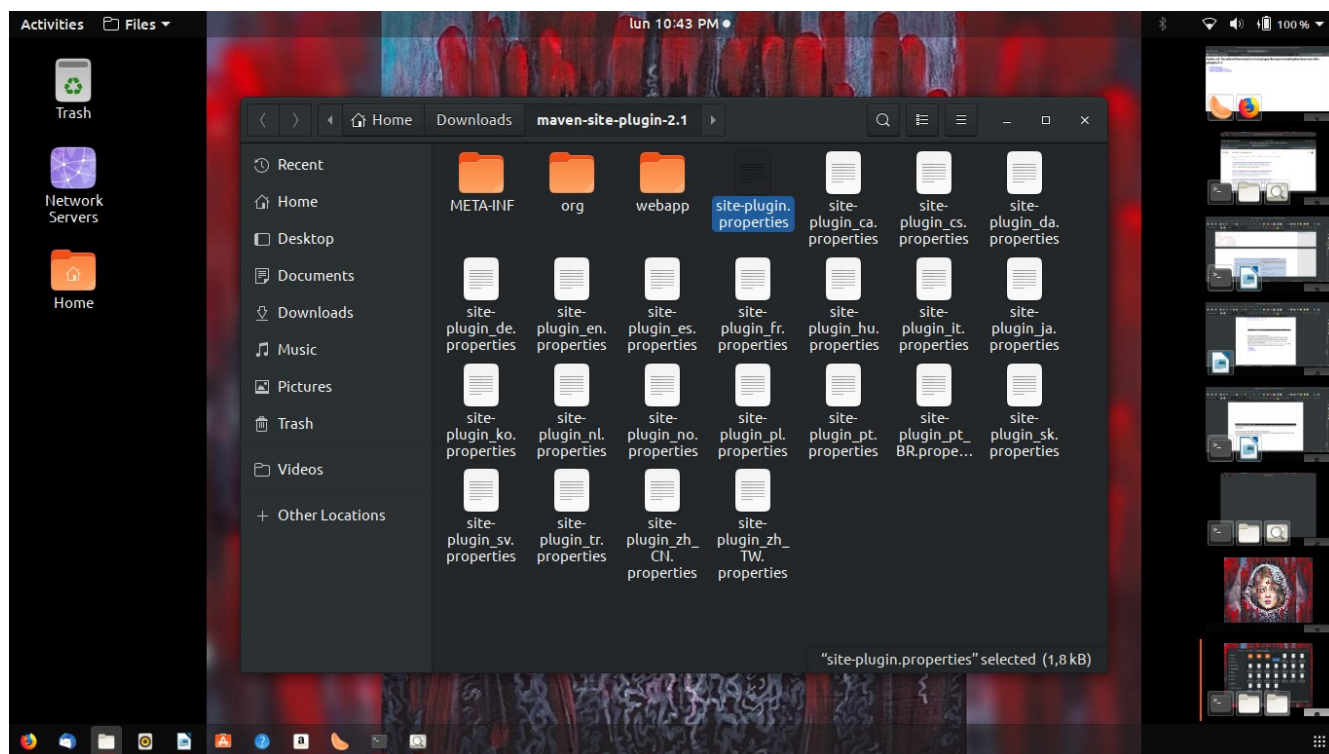
en esta búsqueda, aparecen directorios parecidos a los anteriores, con la diferencia de que ahora se pueden descargar archivos .jar que contienen información sensible del sitio .



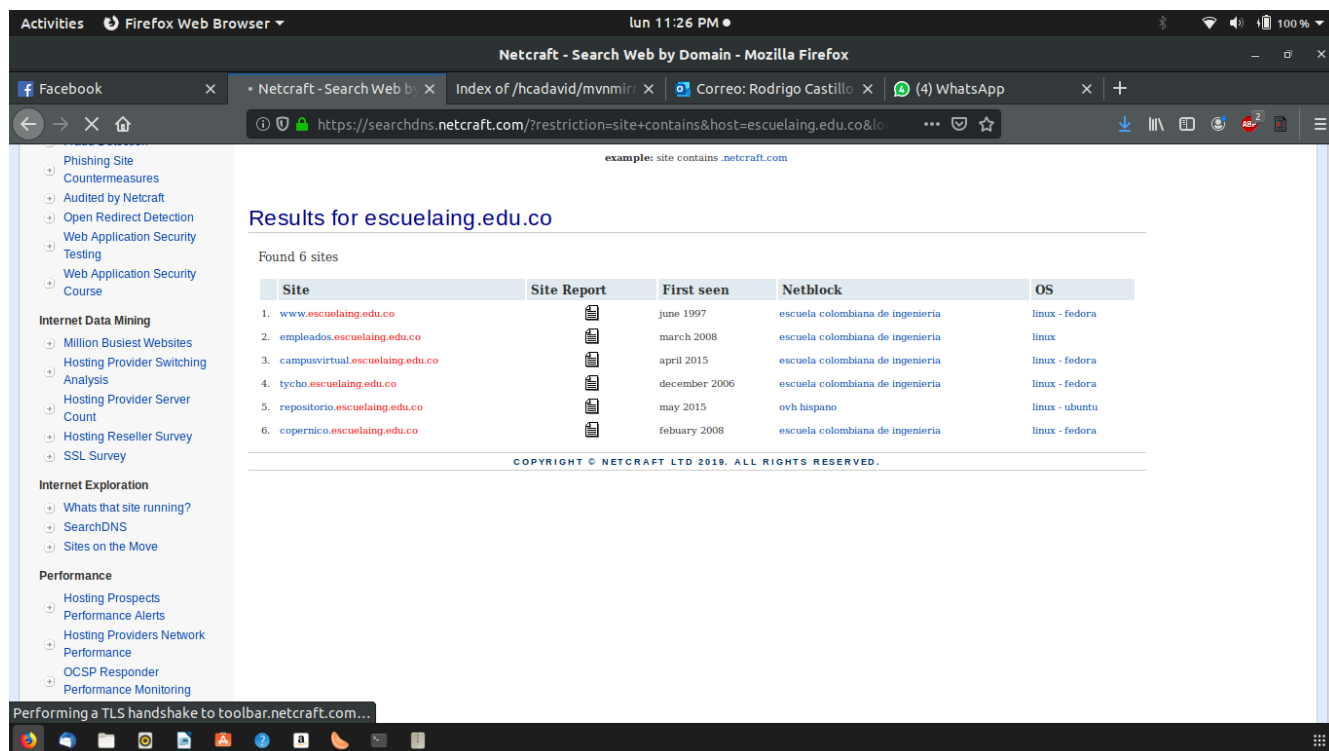
Index of /hcadavid/mvnmirror/org/apache/maven/plugins/maven-site-plugin/2.1

- [Parent Directory](#)
- [maven-site-plugin-2.1.jar](#)
- [maven-site-plugin-2.1.jar.sha1](#)





Segunda Parte: Netcraft



En netcraft podemos encontrar información referente a los servidores de la pagina , acerca del administrador de la pagina, acerca de los ips de los dominios de los servidores de la pagina, los sistemas operativos que usan y sus revisiones, esta información puede ser útil para encontrar servidores desactualizados y vulnerabilidades en ellos

Site report for www.escuelaing.edu.co - Mozilla Firefox

https://toolbar.netcraft.com/site_report?url=http://www.escuelaing.edu.co

Organisation
Registrant Organization: Escuela Colombiana de Ingenieria, Registrant State/Province: Bogota, Registrant Country: CO

Top Level Domain
Colombia (.edu.co)

Hosting country
CO

Hosting company
unknown

DNS Security Extensions
unknown

Hosting History

Netblock owner	IP address	OS	Web server	Last seen	Refresh
ESCUELA COLOMBIANA DE INGENIERIA BOGOTA	45.239.88.102	Linux	Apache/2.2.22 Fedora	9-Sep-2019	
ESCUELA COLOMBIANA DE INGENIERIA BOGOTA	190.24.150.102	Linux	Apache/2.2.22 Fedora	19-Mar-2017	
ESCUELA COLOMBIANA DE INGENIERIA BOGOTA	190.24.150.68	Linux	Apache-Coyote/1.1	1-Aug-2012	
ETB - Colombia Bogota	190.24.150.68	Linux	Apache-Coyote/1.1	27-Apr-2010	
Interconexion Electrica S.A. ISA Medellin	200.24.7.177	Linux	Apache-Coyote/1.1	5-Jun-2006	
Interconexion Electrica S.A. ISA Medellin	200.24.7.177	Linux	Apache/1.3.26 Unix mod_perl/1.24 ApacheJserv/1.1.2	10-Mar-2005	
Interconexion Electrica S.A. ISA Medellin	200.24.7.177	Linux	Apache/1.3.12 Unix	12-May-2004	
Interconexion Electrica S.A. ISA Medellin	200.24.7.177	Linux	Apache/1.3.12 Unix	25-Jun-2002	
Interconexion Electrica S.A. ISA Medellin	200.24.7.184	-	Apache/1.3.12 Unix	31-Jan-2002	
Interconexion Electrica S.A. ISA Medellin	200.24.7.184	Linux	Apache/1.3.12 Unix PHP/3.0.16	29-May-2001	

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of [rules](https://tools.ietf.org/html/rfc7208). Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see [openspf.org](https://tools.ietf.org/html/rfc7208).

Warning: It appears that this host does not have an SPF record. Setting up an SPF record helps prevent the delivery of forged emails from your domain.

Parte 3: Sublist3r :

Sublist3r es un Script en python desarrollado por Ahmed Aboul-Ela , lo que hace es analizar en distintos sitios como en google, bing, baidu, yahoo...etc para averiguar por los subdominios del dominio objetivo que están abiertos, éstos subdominios a veces pueden ser vulnerables puesto que pueden ser subdominios olvidados que estén desactualizados o tengan fallos de seguridad, como el servidor Zico.

```

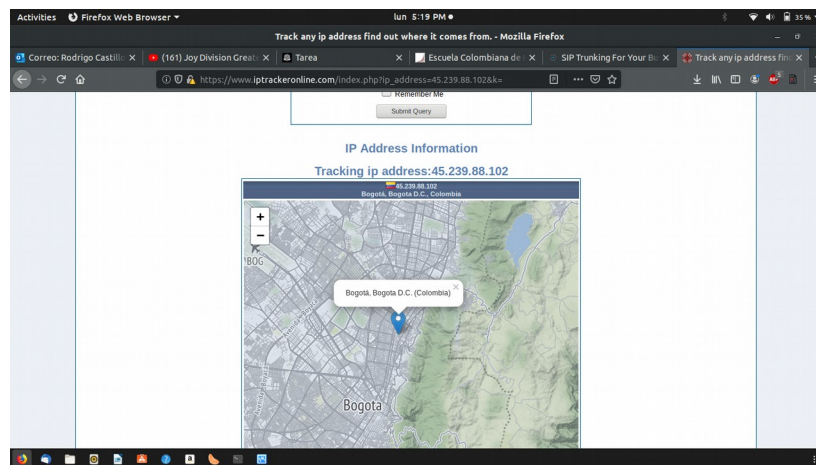
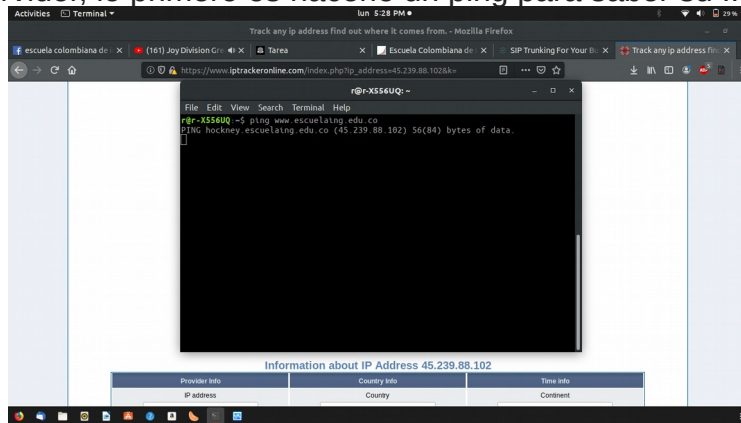
r@r-X556UQ: ~/Documents/Sublist3r
File Edit View Search Terminal Help
estudiantes. escuelaing.edu.co
horarios. escuelaing.edu.co
laboratorio. escuelaing.edu.co
ldn. escuelaing.edu.co
profesores. escuelaing.edu.co
labproduccion. escuelaing.edu.co
landing. escuelaing.edu.co
m. escuelaing.edu.co
notiweb. escuelaing.edu.co
ns2. escuelaing.edu.co
practicas. escuelaing.edu.co
repositorio. escuelaing.edu.co
www. repositorio. escuelaing.edu.co
revistas. escuelaing.edu.co
seda. escuelaing.edu.co
serviciostl. escuelaing.edu.co
tycho. escuelaing.edu.co
tychoi. escuelaing.edu.co
biomedica. urosarto. escuelaing.edu.co
conocimiento. escuelaing.edu.co:8080
estudiantes. escuelaing.edu.co:8087
r@r-X556UQ: ~/Documents/Sublist3r$ ping copernico. escuelaing.edu.co
PING copernico. escuelaing.edu.co (45.239.88.73): 56(84) bytes of data
64 bytes from 45.239.88.73: icmp_seq=1 ttl=56 time=4.85 ms

```

Parte 4: encontrar ubicación del servidor

para encontrar el servidor, lo primero es hacerle un ping para saber su IP

lo segundo es buscar algun localizador de ip en google, para el proposito de este curso, googleé IP-tracker en el buscador para acudir al servicio de alguno de los buscadores online, encontré que el servidor se encuentra ubicado cerca de la iglesia Lourdes, , la 63 con 8va (curiosamente, el servidor de la universidad El Rosario, se encuentra situado en la misma locación , por lo que no es descabellado deducir que ambas universidades acuden al mismo servicio de servidores.



Parte5 : Buscar en redes sociales.

Intenté buscar mediante el motor de búsqueda avanzada sobre gente que trabaja o estudia en la universidad minuto de dios, por ejemplo, busqué los monitores de la sala de sistemas, curiosamente, es gente que tiene amigos en común conmigo en facebook, por lo que, creo que para propósito del curso no tiene sentido, pero podría acudir a mis amigos para adquirir información de los monitores de la sala de sistemas de la universidad.



Parte 6: WebStractor y spadix

Con estas herramientas, es posible acceder a información sobre los empleados de la empresa, por ejemplo, a información de los profesores de la universidad, esta información puede ser útil si se planea un ataque, pues a veces es mas facil atacar a los profesores y hacer ingeniería social.

