Taller 3

Seguridad informática

Presentado a:

Carlos Londoño

Ingeniero de sistemas

Presentado por:

Elkin Ramírez

Yeison Steven castro

Stefany Lorena Sánchez B.

Cartago valle

2 de mayo de 2018

Taller 3

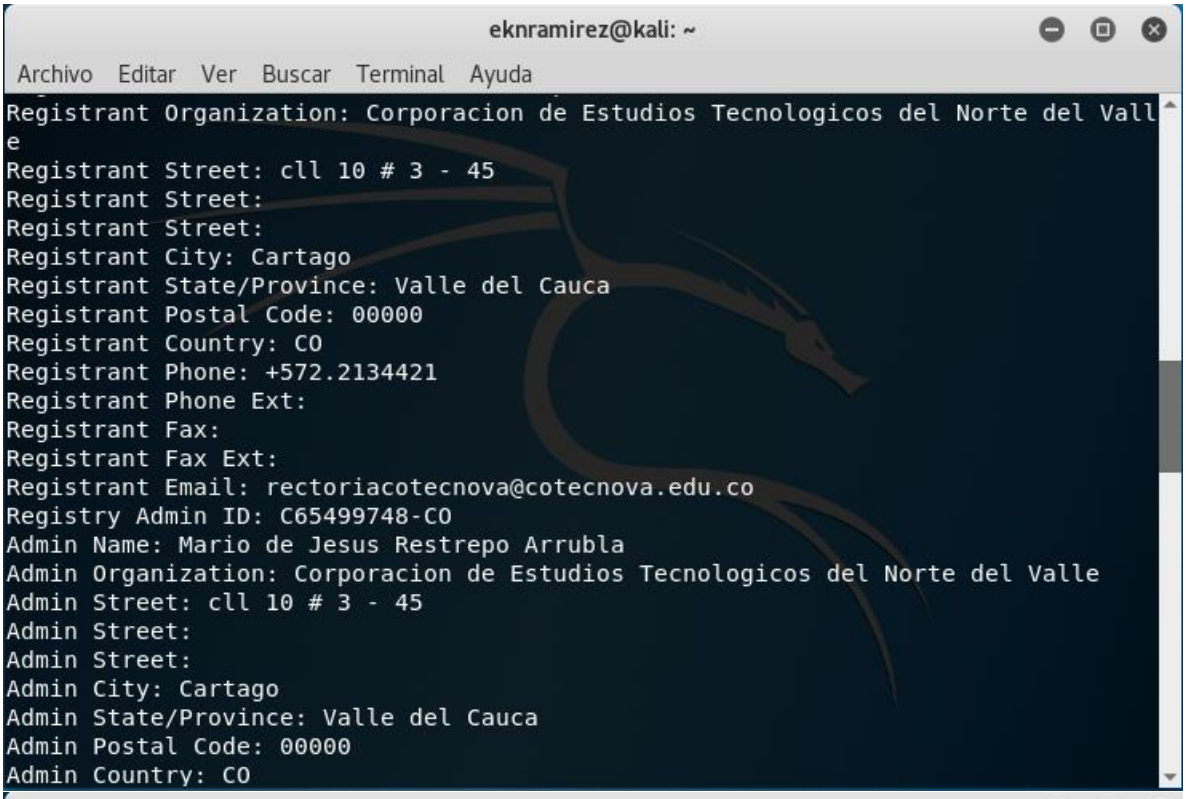
Seguridad Informática

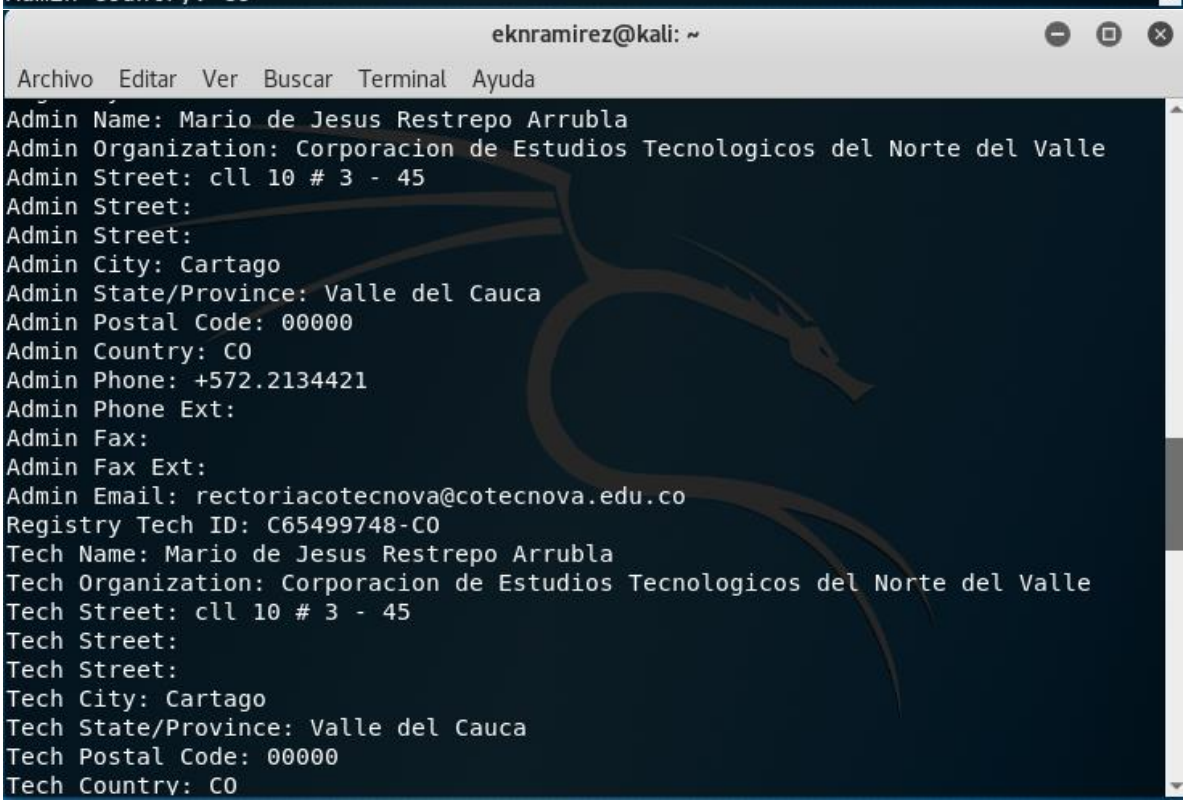
Presentado a Carlos Londoño

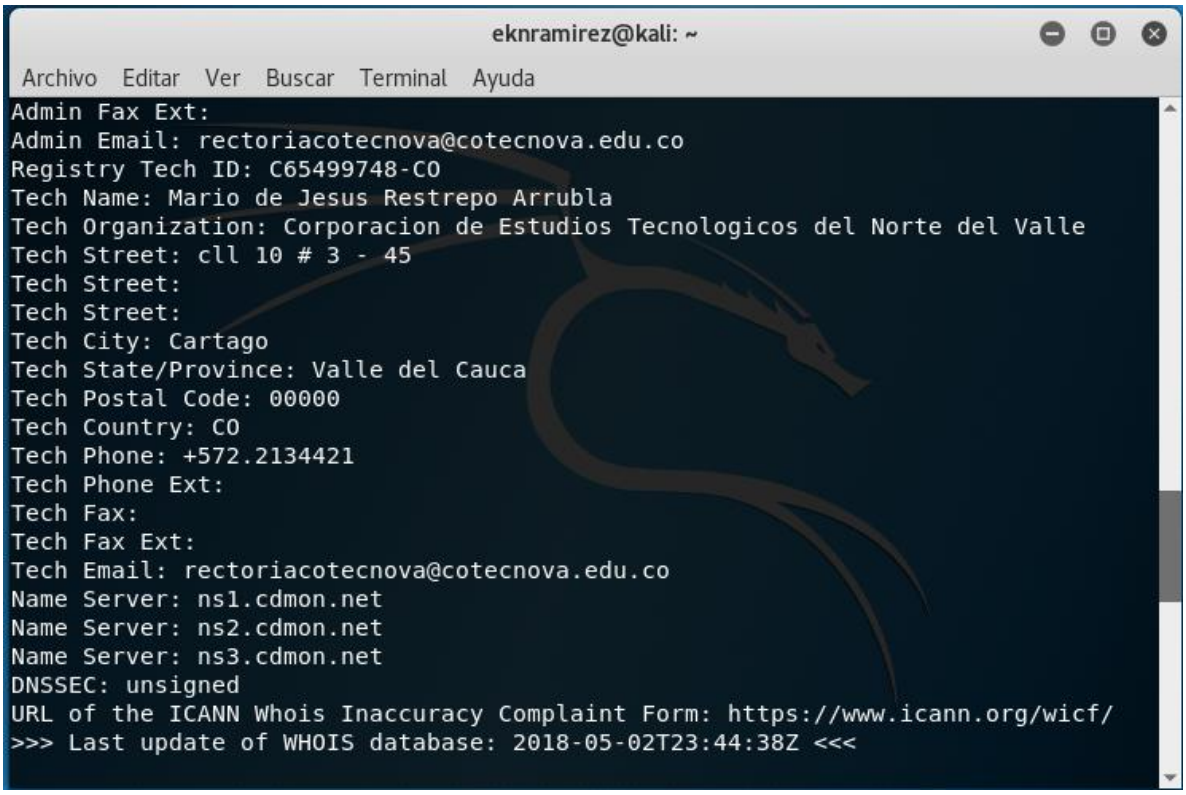
1.) Obtención de Información
   A. Usando el protocolo Whois realizar el análisis del dominio cotecnova.edu.co
   B. Usando el protocolo host realizar el análisis del dominio cotecnova.edu.co
   C. Usando el dominio cotecnova.edu.co usar los siguientes sitios indicando cual es la diferencia de la información que entrega cada uno de ellos. Robtex, IpV4Info.bgp hurricane. Dnsdumpster
   D. Aplicar las técnicas de browser hacking con google y buscar la información disponible de la cotecnova. Edu.co
   E. Aplicando maltego obtener la información del dominio cotecnova.edu.co
   F. Usando recong-ng aplicar un módulo que permita obtener información importante del dominio cotecnova.edu.co
   G. Use theharvester para obtener información adicional a su proceso de investigación de dominio otecnova.edu.co
   H. Consulte archive.org y obtenga información importante sobre las diferentes versiones que ha tenido el dominio cotecnova.edu.co
   I. Usando foca analice por lo menos 3 archivos de dominio cotecnova.edu.co
   J. Resuma en un cuadro comparativo la información más importante que considere que obtuvo de este proceso que le servirá para una auditoria y con que herramienta la obtuvo.
2.) Enumeración de sistemas
   A. Consultar en shodan la información que pueda obtener el dominio cotecnova. educo
   B. Realice un escaneo usando arp, arp-scan, wireshark.
   C. Realizar un escaneo profundo de la red usando la herramienta nmap que permita obtener información importante
   D. Realizar un escaneo profundo de la red usando la herramienta zanmap que permita obtener información importante.
   E. Escanee equipos usandoNC.
   F. Con la herramienta nslookup escanee el dominio cotecnova.edu.co
   G. Aplicar dig y dsmun en el dominio cotecnova.edu.co y comparar la información
   H. Resuma en un cuadro comparativo la información mas importante que considere que obtuvo de este proceso.

3.) Análisis de Vulnerabilidades
   A. Aplicando una herramienta como nessus realice un escaneo de red completo. que me permita obtener información de vulnerabilidades

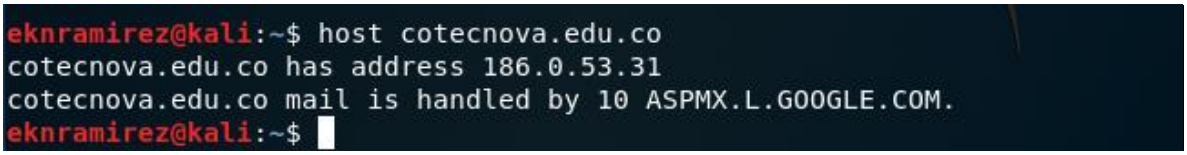
Soluciones del Taller 3





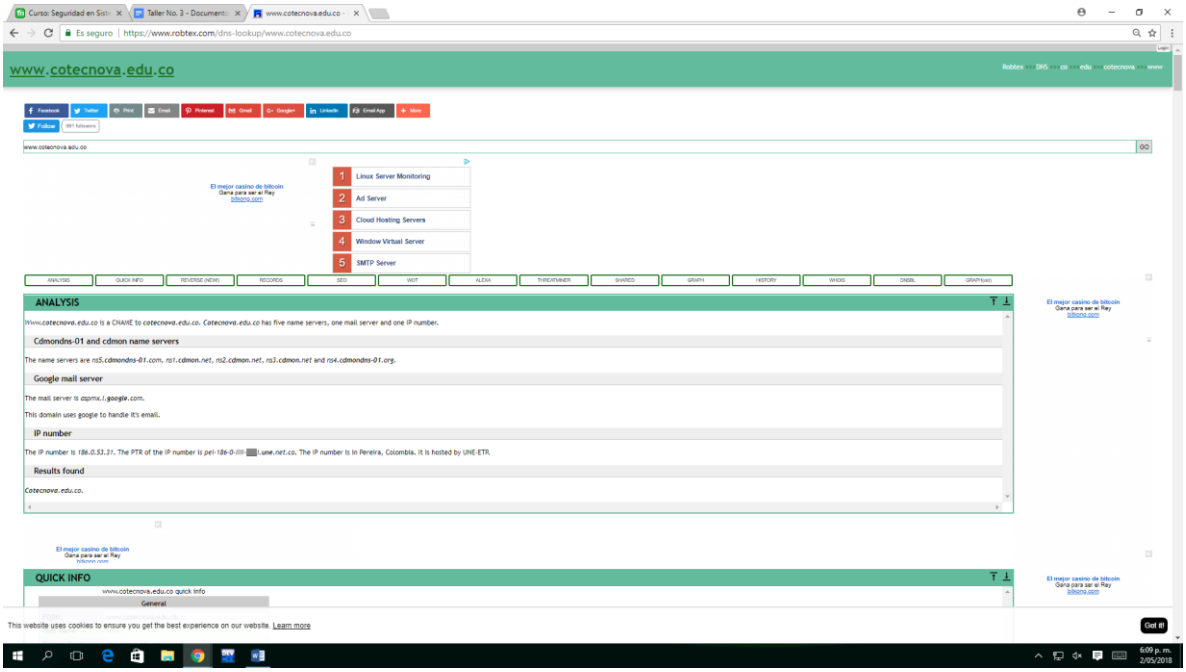


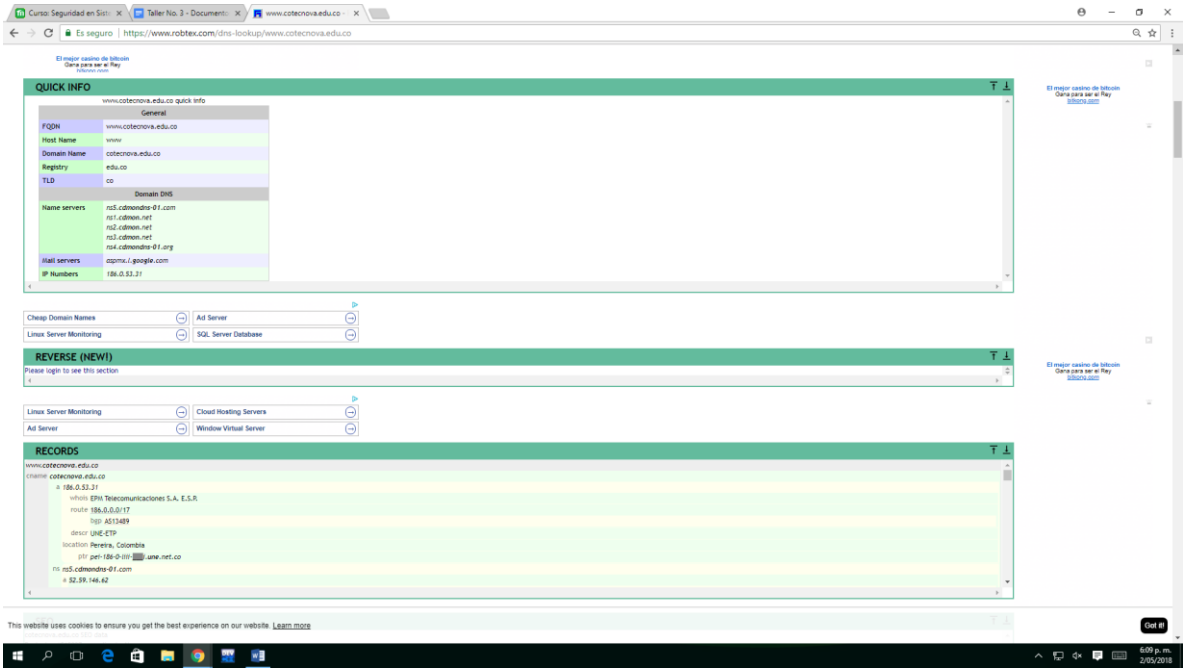
B)

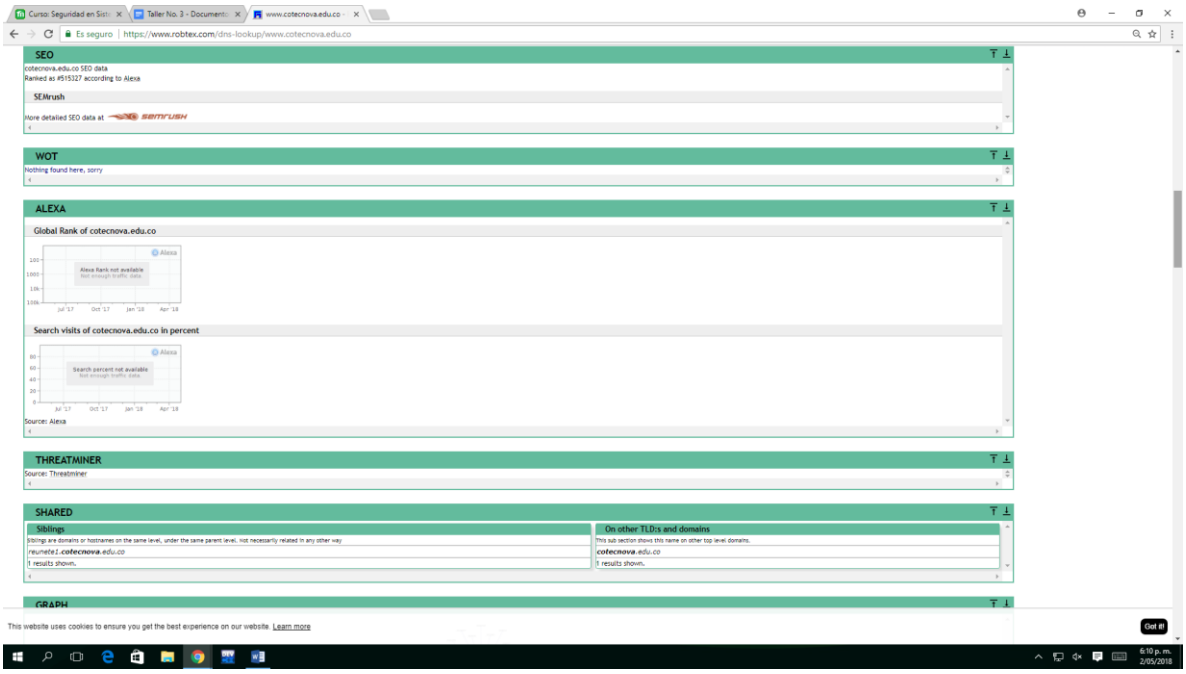


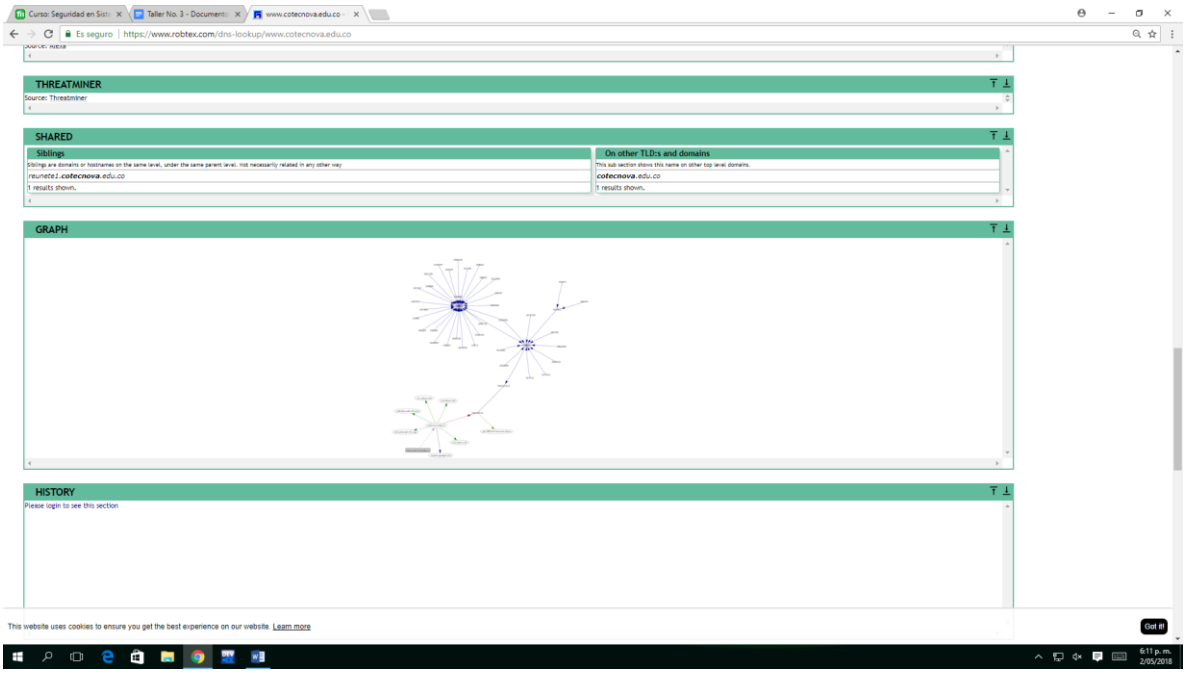
Nos muestra la información de la dirección 1876.0.53.31

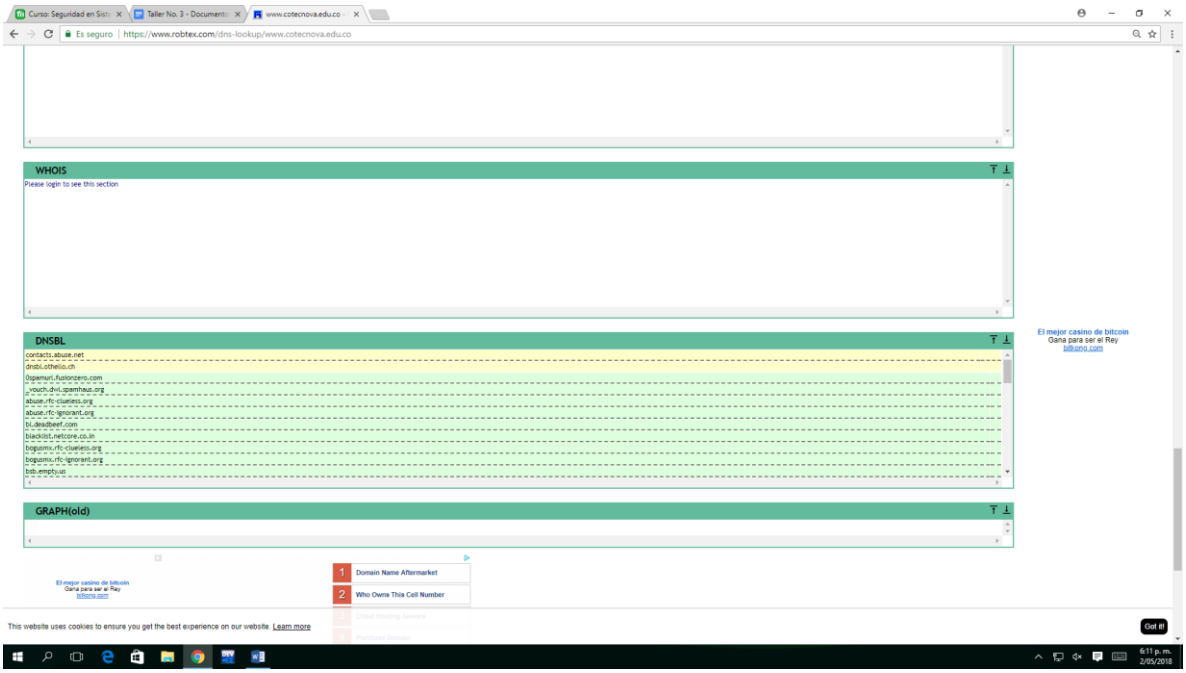
C)


www.cotecnova.edu.co
1 Linux Server Monitoring
2 Ad Server
3 Cloud Hosting Servers
4 Window Virtual Server
5 SMTP Server
ANALYSIS
Cdmondns-01 and cdmon name servers
Google mail server
IP number
Results found
QUICK INFO
This website uses cookies to ensure you get the best experience on our website. Learn more
Got it!

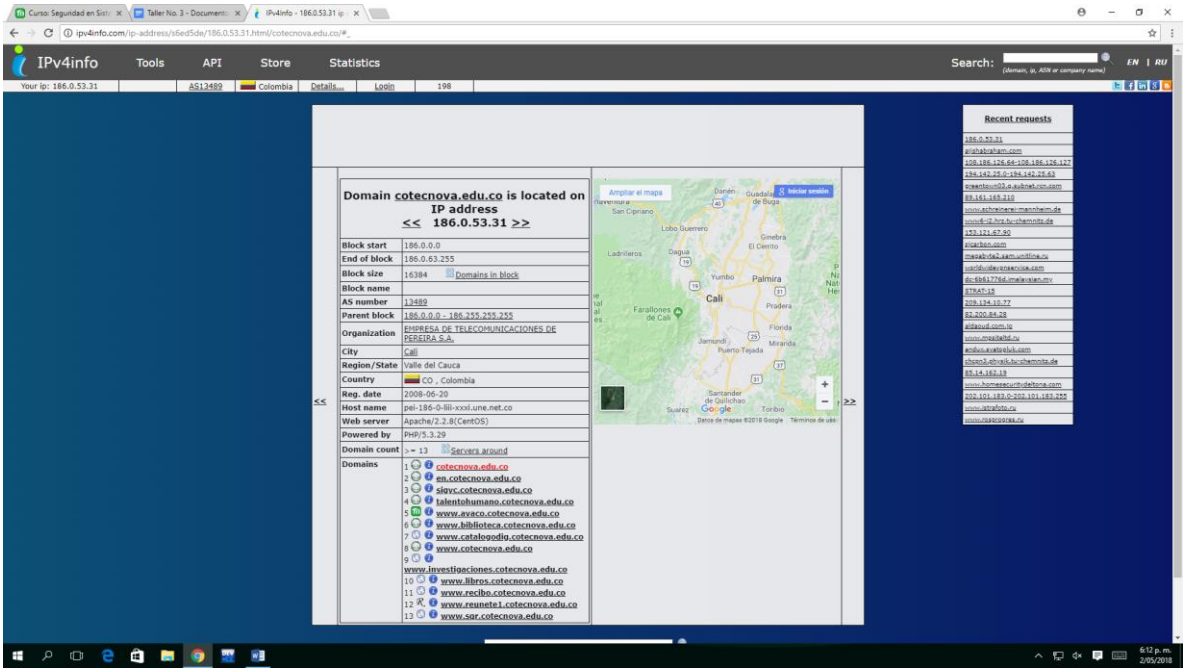

QUICK INFO
General
FQDN www.cotecnova.edu.co
Host Name www
Domain Name cotecnova.edu.co
Registry edu.co
TLD co
Domain DNS
Name servers ns5.cdmondns-01.com
ns1.cdmon.net
ns2.cdmon.net
ns3.cdmon.net
ns4.cdmondns-01.org
Mail servers aspmx.l.google.com
IP Numbers 186.0.53.31
Cheap Domain Names
Ad Server
Linux Server Monitoring
SQL Server Database
REVERSE (NEW!)
Please login to see this section
Linux Server Monitoring
Cloud Hosting Servers
Ad Server
Window Virtual Server
RECORDS
This website uses cookies to ensure you get the best experience on our website. Learn more
Got it!


Curso: Seguridad en Sist
Taller No. 3 - Document
www.cotecnova.edu.co
Es seguro | https://www.robtex.com/dns-lookup/www.cotecnova.edu.co
SEO
cotecnova.edu.co SEO data
Ranked as #515327 according to Alexa
SEMrush
More detailed SEO data at SEMRUSH
WOT
Nothing found here, sorry
ALEXA
Global Rank of cotecnova.edu.co
Alexa Rank not available
Not enough traffic data
Search visits of cotecnova.edu.co in percent
Search percent not available
Not enough traffic data
Source: Alexa
THREATMINER
Source: Threatminer
SHARED
Siblings
Siblings are domains or hostnames on the same level, under the same parent level. Not necessarily related in any other way
reunete1.cotecnova.edu.co
1 results shown.
On other TLD's and domains
This sub section shows this name on other top level domains.
cotecnova.edu.co
1 results shown.
GRAPH
This website uses cookies to ensure you get the best experience on our website. Learn more
Got it!
6:10 p. m.
2/05/2018


Curso: Seguridad en Sist
Taller No. 3 - Document
www.cotecnova.edu.co
Es seguro | https://www.robtex.com/dns-lookup/www.cotecnova.edu.co
THREATMINER
Source: Threatminer
SHARED
Siblings
Siblings are domains or hostnames on the same level, under the same parent level. Not necessarily related in any other way
reunete1.cotecnova.edu.co
1 results shown.
On other TLD's and domains
This sub section shows this name on other top level domains.
cotecnova.edu.co
1 results shown.
GRAPH
HISTORY
Please login to see this section
This website uses cookies to ensure you get the best experience on our website. Learn more
Got it!
6:11 p. m.
2/05/2018



La aplicación Robtex nos muestra información detallada por medio del dominio web, podemos observar unas series de grafos para poder entender de forma gráfica las conexiones de la red.

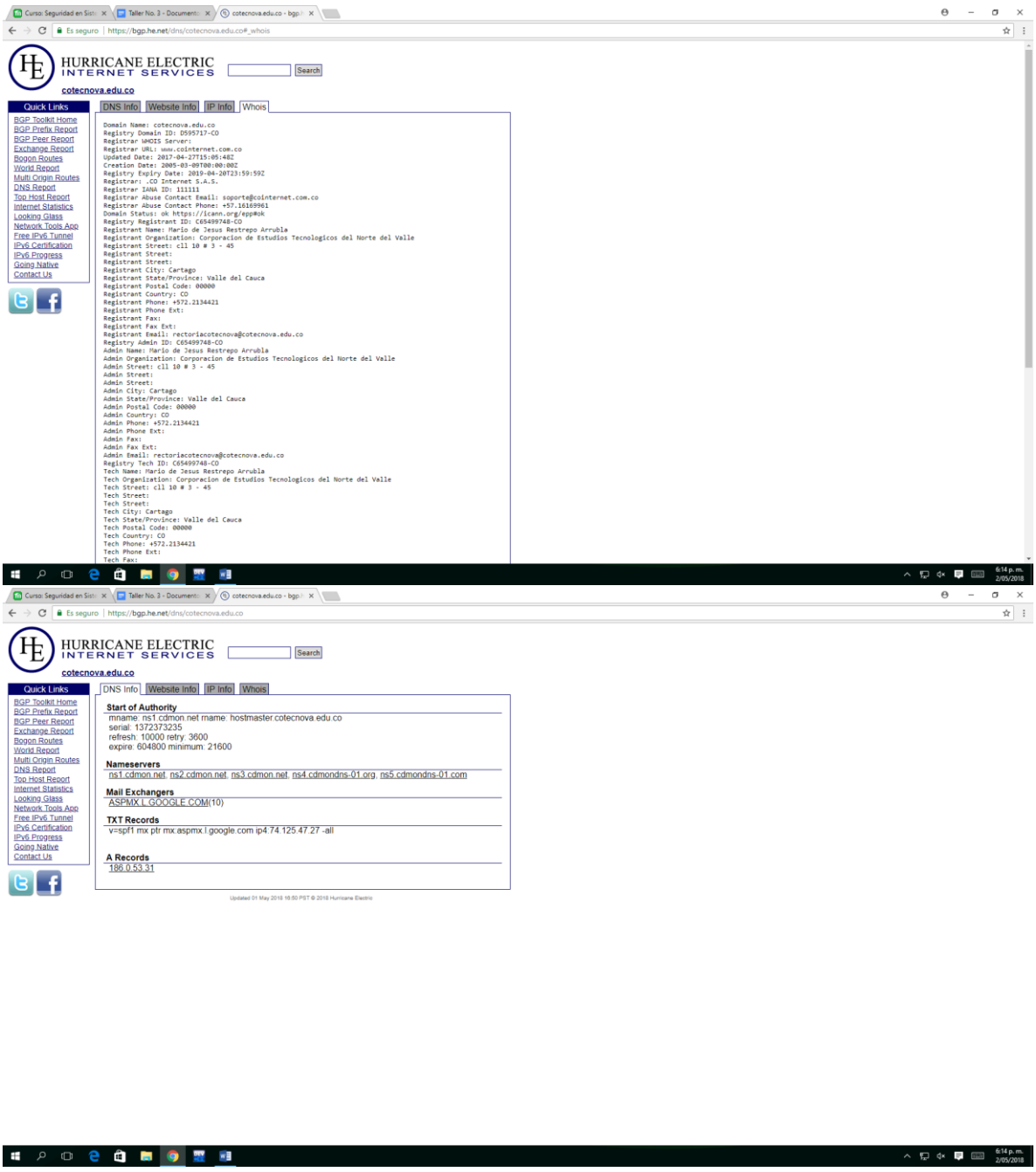


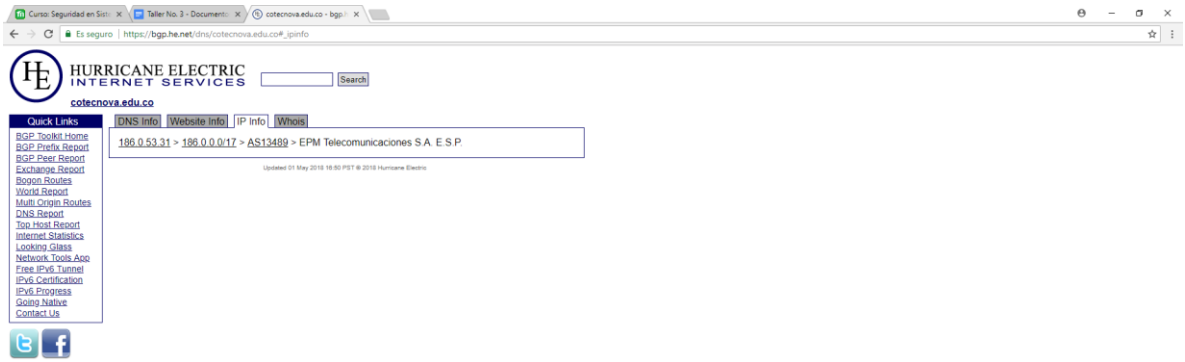
IpV4info.com

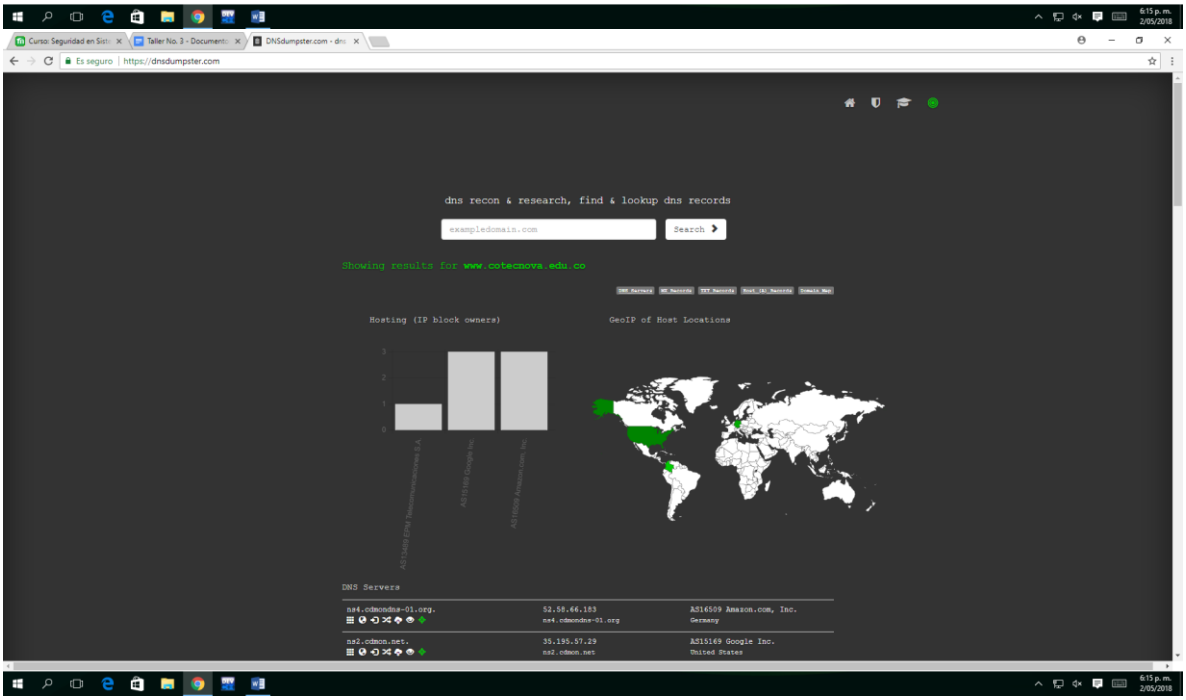
Nos muestra información importante como país. Empresa que presta el servicio de telecomunicaciones en este caso Telecomunicaciones de Pereira

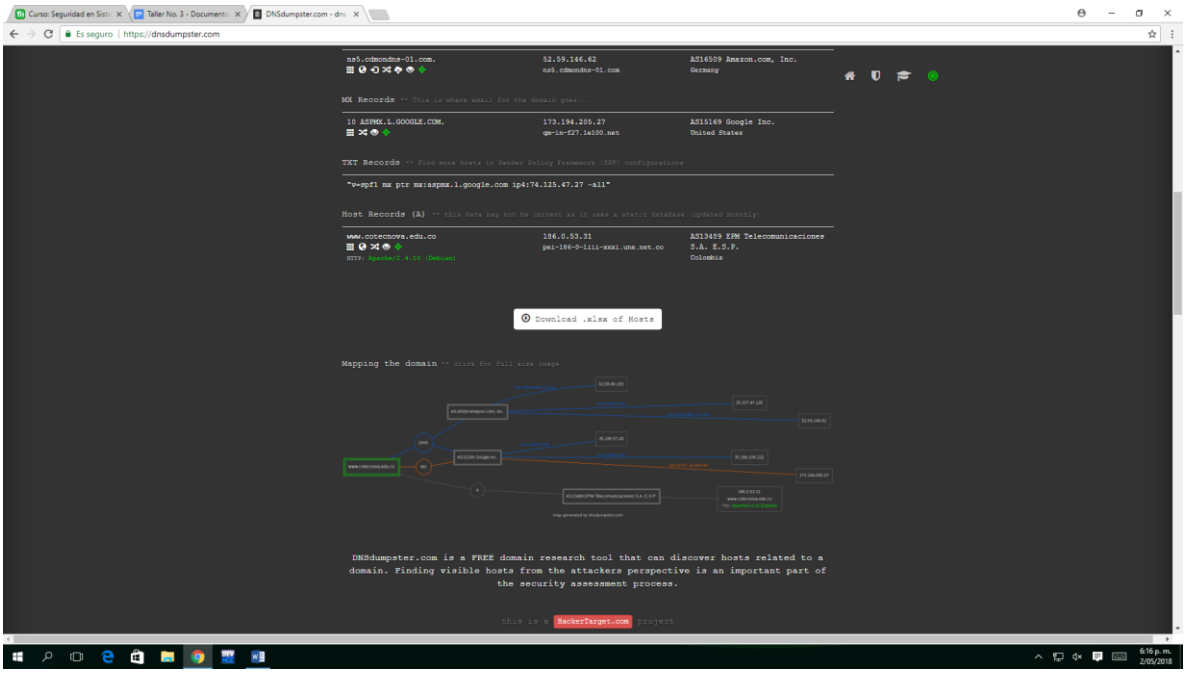
Nos muestra el modelo de servidor en su caso apache.

Muestra subdominios los cuales están en la página

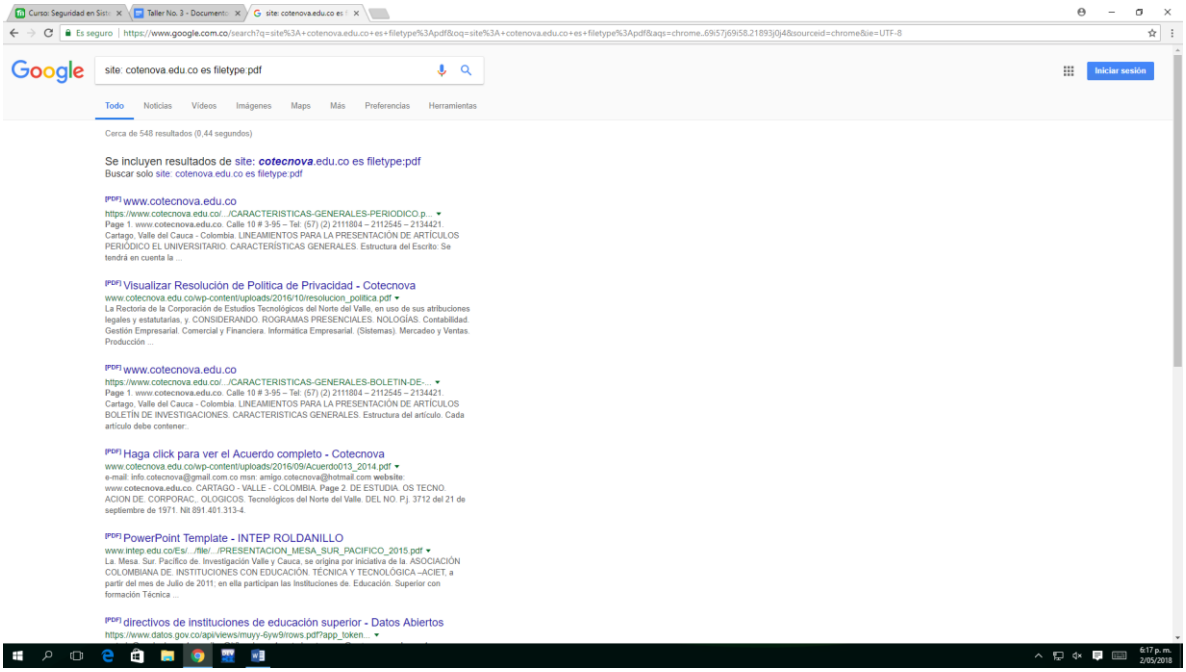


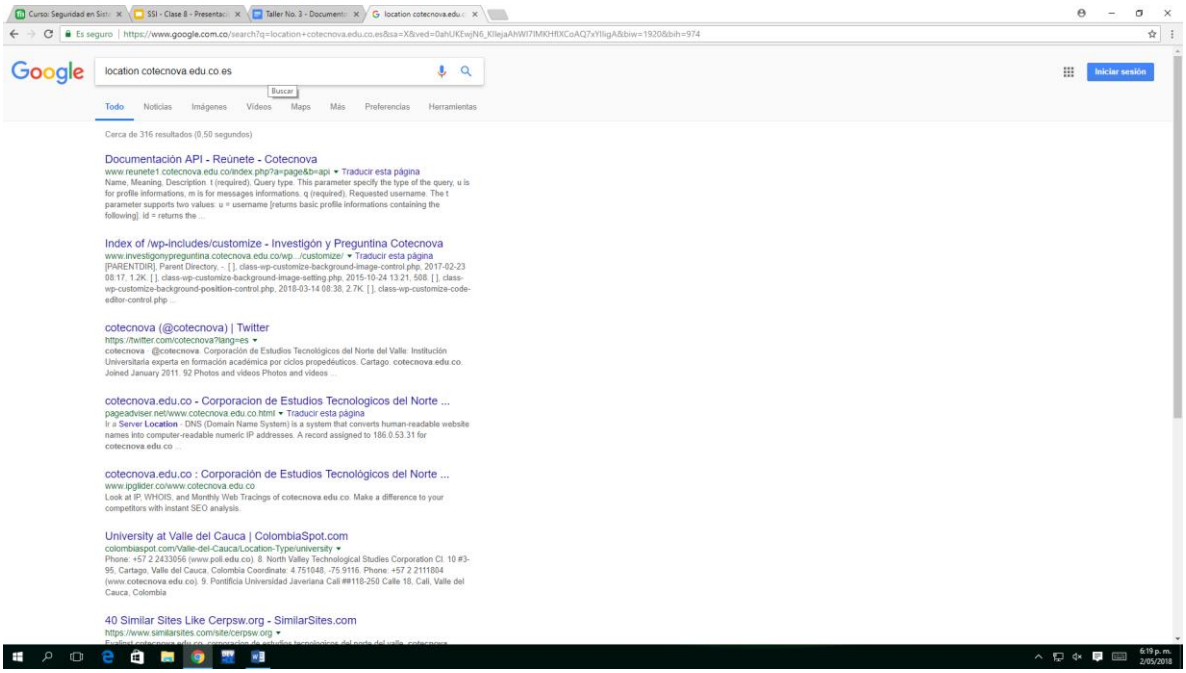

HURRICANE ELECTRIC
INTERNET SERVICES
Search
cotecnova.edu.co
Quick Links
BGP Toolkit Home
BGP Prefix Report
BGP Peer Report
Exchange Report
Bogon Routes
World Report
Multi Origin Routes
DNS Report
Top Host Report
Internet Statistics
Looking Glass
Network Tools App
Free IPv6 Tunnel
IPv6 Certification
IPv6 Progress
Going Native
Contact Us
DNS Info
Website Info
IP Info
Whois
186.0.53.31 > 186.0.0.0/17 > AS13489 > EPM Telecomunicaciones S.A. E.S.P


dns recon & research, find & lookup dns records
exampledomain.com
Search
Showing results for www.cotecnova.edu.co
Hosting (IP block owners)
GeoIP of Host Locations
DNS Servers
ns4.odmondns-01.org.
52.58.66.183
ns4.odmondns-01.org
AS16509 Amazon.com, Inc.
Germany
ns2.odmon.net.
35.195.57.29
ns2.odmon.net
AS15169 Google Inc.
United States


DNSdumpster.com - dns
https://dnsdumpster.com
ns6.cdmondns-01.com.
52.59.146.62
ns6.cdmondns-01.com
AS16509 Amazon.com, Inc.
Germany
MX Records
10 ASPMX.L.GOOGLE.COM.
173.194.205.27
qm-in-f27.1e100.net
AS15169 Google Inc.
United States
TXT Records
"v=spf1 mx ptr mx:aspmx.l.google.com ip4:74.125.47.27 -all"
Host Records (A)
www.cotecnova.edu.co
186.0.53.31
pel-186-0-lili-xxx1.une.net.co
AS13489 EPM Telecomunicaciones S.A. E.S.P.
Colombia
Download .xlsx of Hosts
Mapping the domain
DNSdumpster.com is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process.
this is a HackerTarget.com project

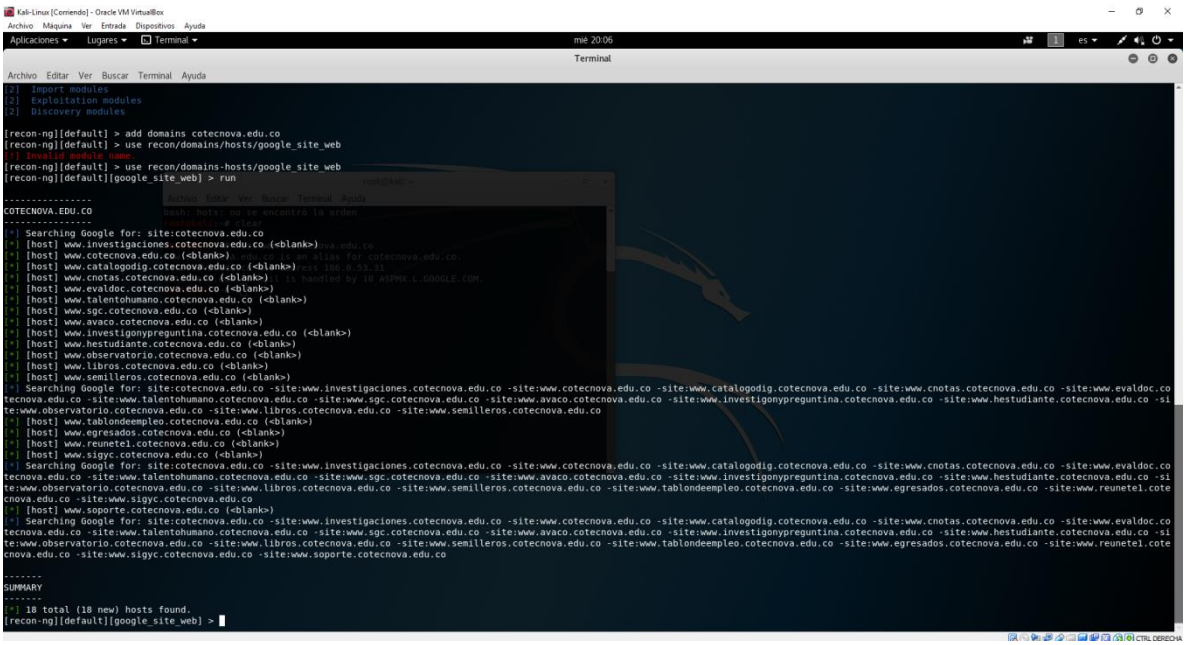
D)


site: cotenova.edu.co es filetype:pdf
https://www.google.com.co/search?q=site%3A+cotenova.edu.co+es+filetype%3Apdf&oq=site%3A+cotenova.edu.co+es+filetype%3Apdf
Google
site: cotenova.edu.co es filetype:pdf
Iniciar sesión
Todo
Noticias
Vídeos
Imágenes
Maps
Más
Preferencias
Herramientas
Cerca de 548 resultados (0,44 segundos)
Se incluyen resultados de site: cotecnova.edu.co es filetype:pdf
Buscar solo site: cotenova.edu.co es filetype:pdf
[PDF] www.cotecnova.edu.co
https://www.cotecnova.edu.co/.../CARACTERISTICAS-GENERALES-PERIODICO.p...
Page 1. www.cotecnova.edu.co. Calle 10 # 3-95 – Tel: (57) (2) 2111804 – 2112545 – 2134421. Cartago, Valle del Cauca - Colombia. LINEAMIENTOS PARA LA PRESENTACIÓN DE ARTÍCULOS PERIÓDICO EL UNIVERSITARIO. CARACTERÍSTICAS GENERALES. Estructura del Escrito. Se tendrá en cuenta la ...
[PDF] Visualizar Resolución de Política de Privacidad - Cotecnova
www.cotecnova.edu.co/wp-content/uploads/2016/10/resolucion_politica.pdf
La Rectoría de la Corporación de Estudios Tecnológicos del Norte del Valle, en uso de sus atribuciones legales y estatutarias, y. CONSIDERANDO. ROGRAMAS PRESENCIALES. NOLOGÍAS. Contabilidad. Gestión Empresarial. Comercial y Financiera. Informática Empresarial. (Sistemas). Mercadeo y Ventas. Producción ...
[PDF] www.cotecnova.edu.co
https://www.cotecnova.edu.co/.../CARACTERISTICAS-GENERALES-BOLETIN-DE-...
Page 1. www.cotecnova.edu.co. Calle 10 # 3-95 – Tel: (57) (2) 2111804 – 2112545 – 2134421. Cartago, Valle del Cauca - Colombia. LINEAMIENTOS PARA LA PRESENTACIÓN DE ARTÍCULOS BOLETÍN DE INVESTIGACIONES. CARACTERÍSTICAS GENERALES. Estructura del artículo. Cada artículo debe contener:
[PDF] Haga click para ver el Acuerdo completo - Cotecnova
www.cotecnova.edu.co/wp-content/uploads/2016/09/Acuerdo013_2014.pdf
e-mail: info.cotecnova@gmail.com.co msn: amigo.cotecnova@hotmail.com website: www.cotecnova.edu.co. CARTAGO - VALLE - COLOMBIA. Page 2. DE ESTUDIA. OS TECNO. ACION DE. CORPORAC,. OLOGICOS. Tecnológicos del Norte del Valle. DEL NO. P.J. 3712 del 21 de septiembre de 1971. Nit.891.401.313-4.
[PDF] PowerPoint Template - INTEP ROLDANILLO
www.intep.edu.co/Es/.../file/.../PRESENTACION_MESA_SUR_PACIFICO_2015.pdf
La. Mesa. Sur. Pacífico de. Investigación Valle y Cauca, se origina por iniciativa de la. ASOCIACIÓN COLOMBIANA DE. INSTITUCIONES CON EDUCACIÓN. TÉCNICA Y TECNOLÓGICA –ACIET, a partir del mes de Julio de 2011; en ella participan las Instituciones de. Educación. Superior con formación Técnica ...
[PDF] directivos de instituciones de educación superior - Datos Abiertos
https://www.datos.gov.co/api/views/muyy-6yw9/rows.pdf?app_token...

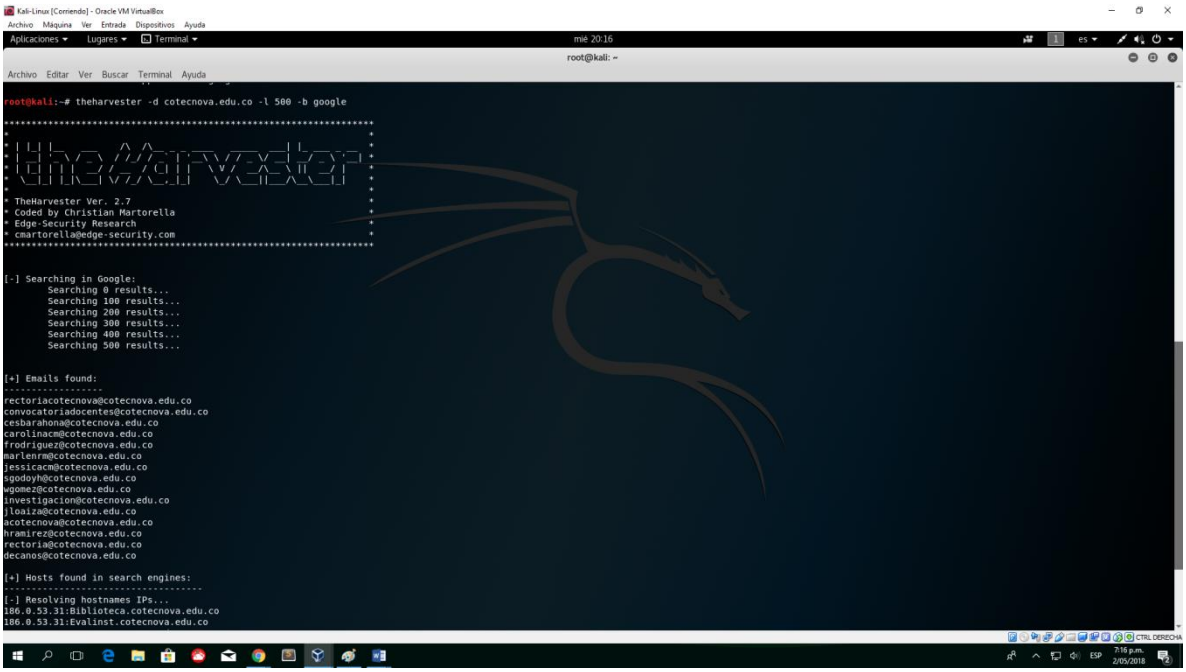

location cotecnova.edu.co es
Buscar
Iniciar sesión
Todo Noticias Imágenes Vídeos Maps Más Preferencias Herramientas
Cerca de 316 resultados (0,50 segundos)
Documentación API - Reúnete - Cotecnova
www.reunete1.cotecnova.edu.co/index.php?a=page&b=api ▾ Traducir esta página
Name. Meaning. Description. t (required). Query type. This parameter specify the type of the query, u is for profile informations; m is for messages informations. q (required). Requested username. The t parameter supports two values: u = username [returns basic profile informations containing the following]. id = returns the ...
Index of /wp-includes/customize - Investigón y Preguntina Cotecnova
www.investigonypreguntina.cotecnova.edu.co/wp.../customize/ ▾ Traducir esta página
[PARENTDIR], Parent Directory, -, [], class-wp-customize-background-image-control.php, 2017-02-23 08:17, 1.2K, [], class-wp-customize-background-image-setting.php, 2015-10-24 13:21, 508, [], class-wp-customize-background-position-control.php, 2018-03-14 08:38, 2.7K, [], class-wp-customize-code-editor-control.php ...
cotecnova (@cotecnova) | Twitter
https://twitter.com/cotecnova?lang=es ▾
cotecnova · @cotecnova. Corporación de Estudios Tecnológicos del Norte del Valle. Institución Universitaria experta en formación académica por ciclos propedéuticos. Cartago. cotecnova.edu.co. Joined January 2011. 92 Photos and videos Photos and videos ...
cotecnova.edu.co - Corporacion de Estudios Tecnologicos del Norte ...
pageadviser.net/www.cotecnova.edu.co.html ▾ Traducir esta página
Ir a Server Location - DNS (Domain Name System) is a system that converts human-readable website names into computer-readable numeric IP addresses. A record assigned to 186.0.53.31 for cotecnova.edu.co ...
cotecnova.edu.co : Corporación de Estudios Tecnológicos del Norte ...
www.ipglider.co/www.cotecnova.edu.co
Look at IP, WHOIS, and Monthly Web Tracings of cotecnova.edu.co. Make a difference to your competitors with instant SEO analysis.
University at Valle del Cauca | ColombiaSpot.com
colombiaspot.com/Valle-del-Cauca/Location-Type/university ▾
Phone: +57 2 2433056 (www.poli.edu.co). 8. North Valley Technological Studies Corporation Cl. 10 #3-95, Cartago, Valle del Cauca, Colombia Coordinate: 4.751048, -75.9116. Phone: +57 2 2111804 (www.cotecnova.edu.co). 9. Pontificia Universidad Javeriana Cali ##118-250 Calle 18, Cali, Valle del Cauca, Colombia
40 Similar Sites Like Cerpsw.org - SimilarSites.com
https://www.similarsites.com/site/cerpsw.org ▾

e)

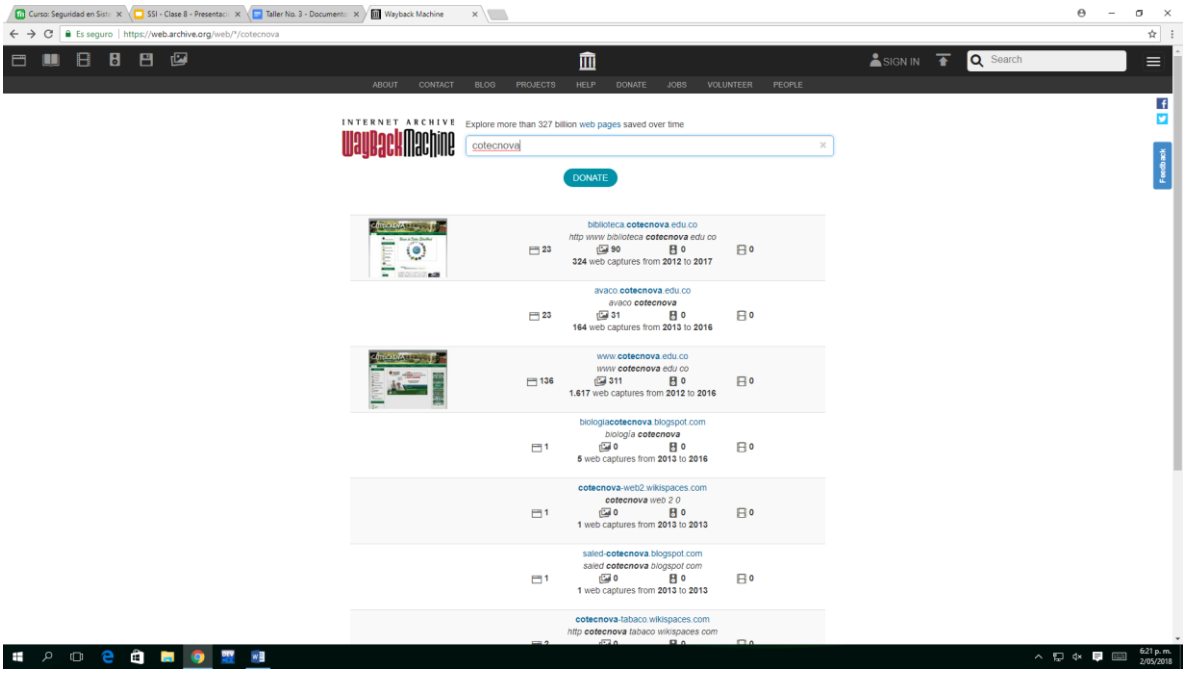
f)

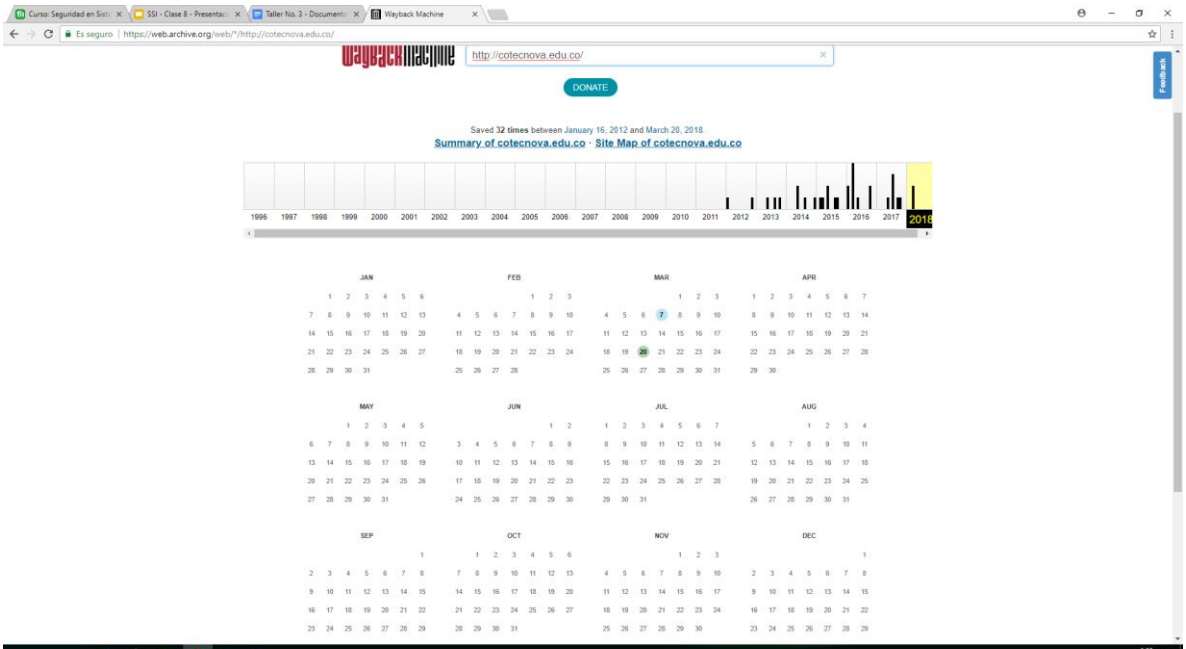

Kali-Linux [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Lugares Terminal
mié 20:06
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
[2] Import modules
[2] Exploitation modules
[2] Discovery modules
[recon-ng][default] > add domains cotecnova.edu.co
[recon-ng][default] > use recon/domains/hosts/google_site_web
[!] Invalid module name.
[recon-ng][default] > use recon/domains-hosts/google_site_web
[recon-ng][default][google_site_web] > run
COTECNOVA.EDU.CO
[*] Searching Google for: site:cotecnova.edu.co
[*] [host] www.investigaciones.cotecnova.edu.co (<blank>)
[*] [host] www.cotecnova.edu.co (<blank>)
[*] [host] www.catalogodig.cotecnova.edu.co (<blank>)
[*] [host] www.cnotas.cotecnova.edu.co (<blank>)
[*] [host] www.evaldoc.cotecnova.edu.co (<blank>)
[*] [host] www.talentohumano.cotecnova.edu.co (<blank>)
[*] [host] www.sgc.cotecnova.edu.co (<blank>)
[*] [host] www.avaco.cotecnova.edu.co (<blank>)
[*] [host] www.investigonypreguntina.cotecnova.edu.co (<blank>)
[*] [host] www.hestudiante.cotecnova.edu.co (<blank>)
[*] [host] www.observatorio.cotecnova.edu.co (<blank>)
[*] [host] www.libros.cotecnova.edu.co (<blank>)
[*] [host] www.semilleros.cotecnova.edu.co (<blank>)
[*] Searching Google for: site:cotecnova.edu.co -site:www.investigaciones.cotecnova.edu.co -site:www.cotecnova.edu.co -site:www.catalogodig.cotecnova.edu.co -site:www.cnotas.cotecnova.edu.co -site:www.evaldoc.cotecnova.edu.co -site:www.talentohumano.cotecnova.edu.co -site:www.sgc.cotecnova.edu.co -site:www.avaco.cotecnova.edu.co -site:www.investigonypreguntina.cotecnova.edu.co -site:www.hestudiante.cotecnova.edu.co -site:www.observatorio.cotecnova.edu.co -site:www.libros.cotecnova.edu.co -site:www.semilleros.cotecnova.edu.co
[*] [host] www.tablondeempleo.cotecnova.edu.co (<blank>)
[*] [host] www.egresados.cotecnova.edu.co (<blank>)
[*] [host] www.reunete1.cotecnova.edu.co (<blank>)
[*] [host] www.sigyc.cotecnova.edu.co (<blank>)
[*] Searching Google for: site:cotecnova.edu.co -site:www.investigaciones.cotecnova.edu.co -site:www.cotecnova.edu.co -site:www.catalogodig.cotecnova.edu.co -site:www.cnotas.cotecnova.edu.co -site:www.evaldoc.cotecnova.edu.co -site:www.talentohumano.cotecnova.edu.co -site:www.sgc.cotecnova.edu.co -site:www.avaco.cotecnova.edu.co -site:www.investigonypreguntina.cotecnova.edu.co -site:www.hestudiante.cotecnova.edu.co -site:www.observatorio.cotecnova.edu.co -site:www.libros.cotecnova.edu.co -site:www.semilleros.cotecnova.edu.co -site:www.tablondeempleo.cotecnova.edu.co -site:www.egresados.cotecnova.edu.co -site:www.reunete1.cotecnova.edu.co -site:www.sigyc.cotecnova.edu.co
[*] [host] www.soporte.cotecnova.edu.co (<blank>)
[*] Searching Google for: site:cotecnova.edu.co -site:www.investigaciones.cotecnova.edu.co -site:www.cotecnova.edu.co -site:www.catalogodig.cotecnova.edu.co -site:www.cnotas.cotecnova.edu.co -site:www.evaldoc.cotecnova.edu.co -site:www.talentohumano.cotecnova.edu.co -site:www.sgc.cotecnova.edu.co -site:www.avaco.cotecnova.edu.co -site:www.investigonypreguntina.cotecnova.edu.co -site:www.hestudiante.cotecnova.edu.co -site:www.observatorio.cotecnova.edu.co -site:www.libros.cotecnova.edu.co -site:www.semilleros.cotecnova.edu.co -site:www.tablondeempleo.cotecnova.edu.co -site:www.egresados.cotecnova.edu.co -site:www.reunete1.cotecnova.edu.co -site:www.sigyc.cotecnova.edu.co -site:www.soporte.cotecnova.edu.co
SUMMARY
[*] 18 total (18 new) hosts found.
[recon-ng][default][google_site_web] >
CTRL DERECHA

G)


Kali-Linux [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Lugares Terminal mié 20:16 es
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# theharvester -d cotecnova.edu.co -l 500 -b google
* TheHarvester Ver. 2.7
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[-] Searching in Google:
Searching 0 results...
Searching 100 results...
Searching 200 results...
Searching 300 results...
Searching 400 results...
Searching 500 results...
[+] Emails found:
rectoriacotecnova@cotecnova.edu.co
convocatoriadocentes@cotecnova.edu.co
cesbarahona@cotecnova.edu.co
carolinacm@cotecnova.edu.co
frodriguez@cotecnova.edu.co
marlenrm@cotecnova.edu.co
jessicacm@cotecnova.edu.co
sgodoyh@cotecnova.edu.co
wgomez@cotecnova.edu.co
investigacion@cotecnova.edu.co
jloaiza@cotecnova.edu.co
acotecnova@cotecnova.edu.co
hramirez@cotecnova.edu.co
rectoria@cotecnova.edu.co
decanos@cotecnova.edu.co
[+] Hosts found in search engines:
[-] Resolving hostnames IPs...
186.0.53.31:Biblioteca.cotecnova.edu.co
186.0.53.31:Evalinst.cotecnova.edu.co

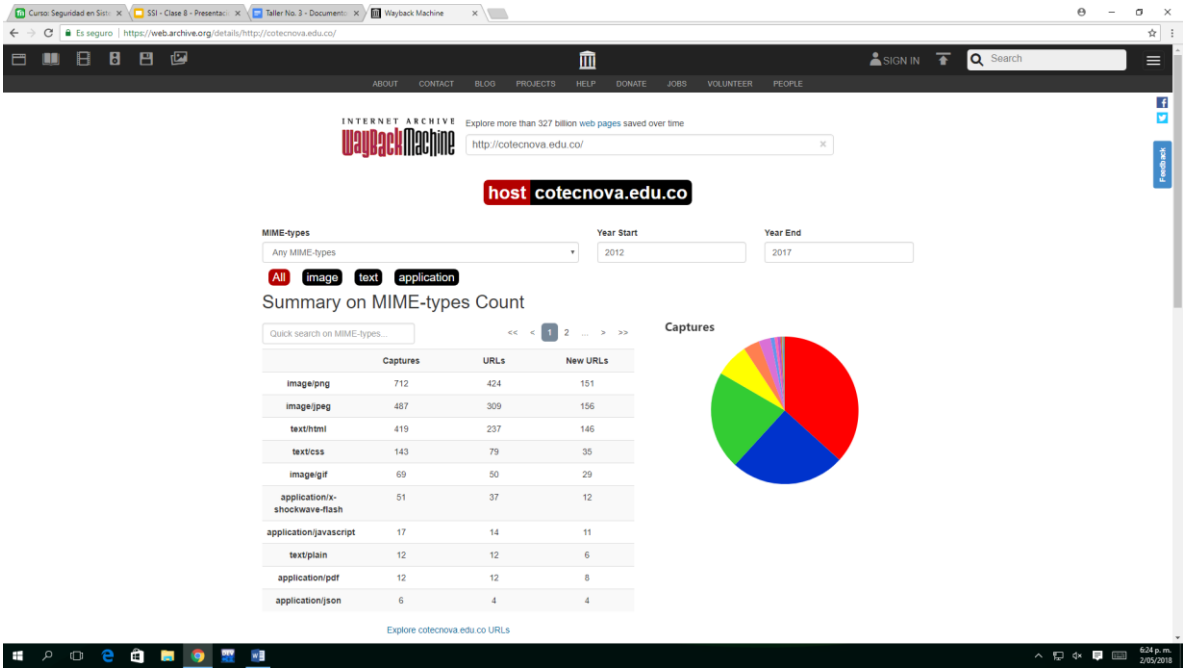
H)


Wayback Machine
https://web.archive.org/web/*/cotecnova
SIGN IN
Search
ABOUT CONTACT BLOG PROJECTS HELP DONATE JOBS VOLUNTEER PEOPLE
INTERNET ARCHIVE
WaybackMachine
Explore more than 327 billion web pages saved over time
cotecnova
DONATE
biblioteca.cotecnova.edu.co
http www.biblioteca.cotecnova.edu.co
90 0
324 web captures from 2012 to 2017
avaco.cotecnova.edu.co
avaco cotecnova
31 0
164 web captures from 2013 to 2016
www.cotecnova.edu.co
www cotecnova edu co
311 0
1.617 web captures from 2012 to 2016
biologiacotecnova.blogspot.com
biologia cotecnova
0 0
5 web captures from 2013 to 2016
cotecnova-web2.wikispaces.com
cotecnova web 2 0
0 0
1 web captures from 2013 to 2013
saled-cotecnova.blogspot.com
saled cotecnova blogspot com
0 0
1 web captures from 2013 to 2013
cotecnova-tabaco.wikispaces.com
http cotecnova tabaco wikispaces com
Feedback


Wayback Machine
http://cotecnova.edu.co/
DONATE
Saved 32 times between January 16, 2012 and March 20, 2018.
Summary of cotecnova.edu.co · Site Map of cotecnova.edu.co
1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018
JAN FEB MAR APR
MAY JUN JUL AUG
SEP OCT NOV DEC


https://web.archive.org/web/20120116230703/http://cotecnova.edu.co/
http://cotecnova.edu.co/
32 captures
JAN 16 2012
COTECNOVA
Corporación de Estudios Tecnológicos del Norte del Valle
Inicio
Quienes Somos
Campus
Programas
Noticias
Biblioteca
GEA-UR
Contáctenos
Información
Aspirantes
Estudiantes
Egresados
Docentes
Padres de Familia
Corporación en Línea
Correo Electrónico
Avaco
LEER MAS
BOLSA DE EMPLEO
CREDITOS FINACIEROS
EL UNIVERSITARIO
GESTION DE CALIDAD
EVENTOS
Calle 10 # 3-95 Tel: 2111804-2112545 Fax: 2134421
Cartago - Valle E-mail: info@cotecnova.edu.co

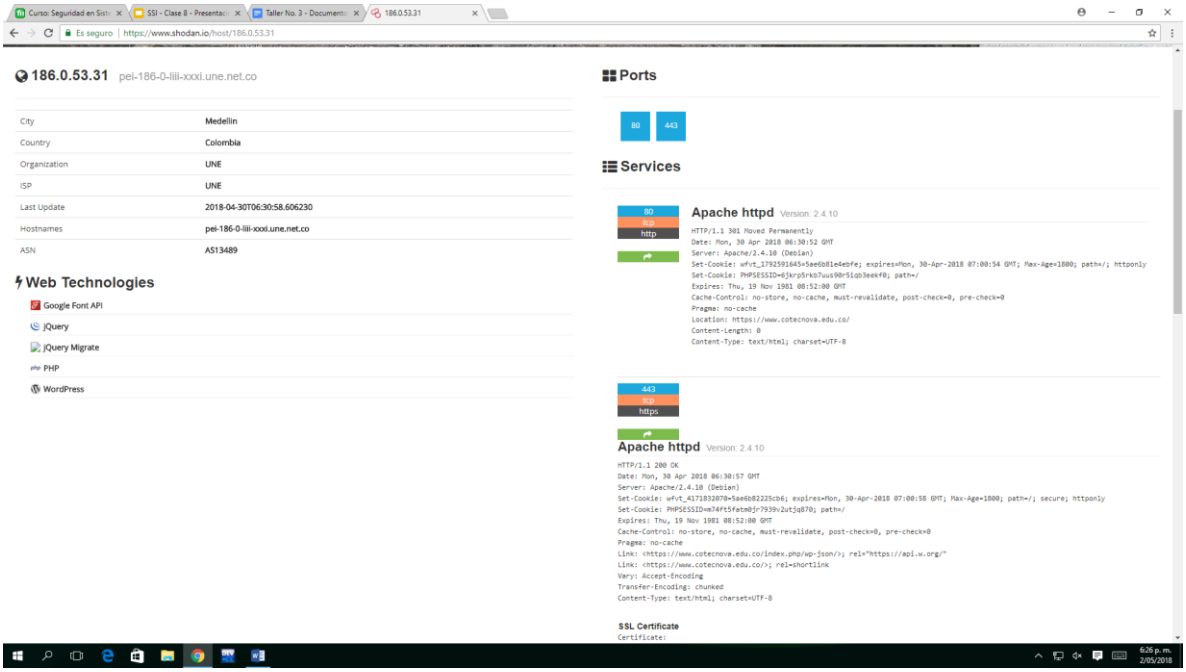
Podemos obervar los diversos cambios que ah sufrido la pagina en cuanto a actualizaciones y mejoras en su aspecto funcional y visual .



Parte del taller 3

2)

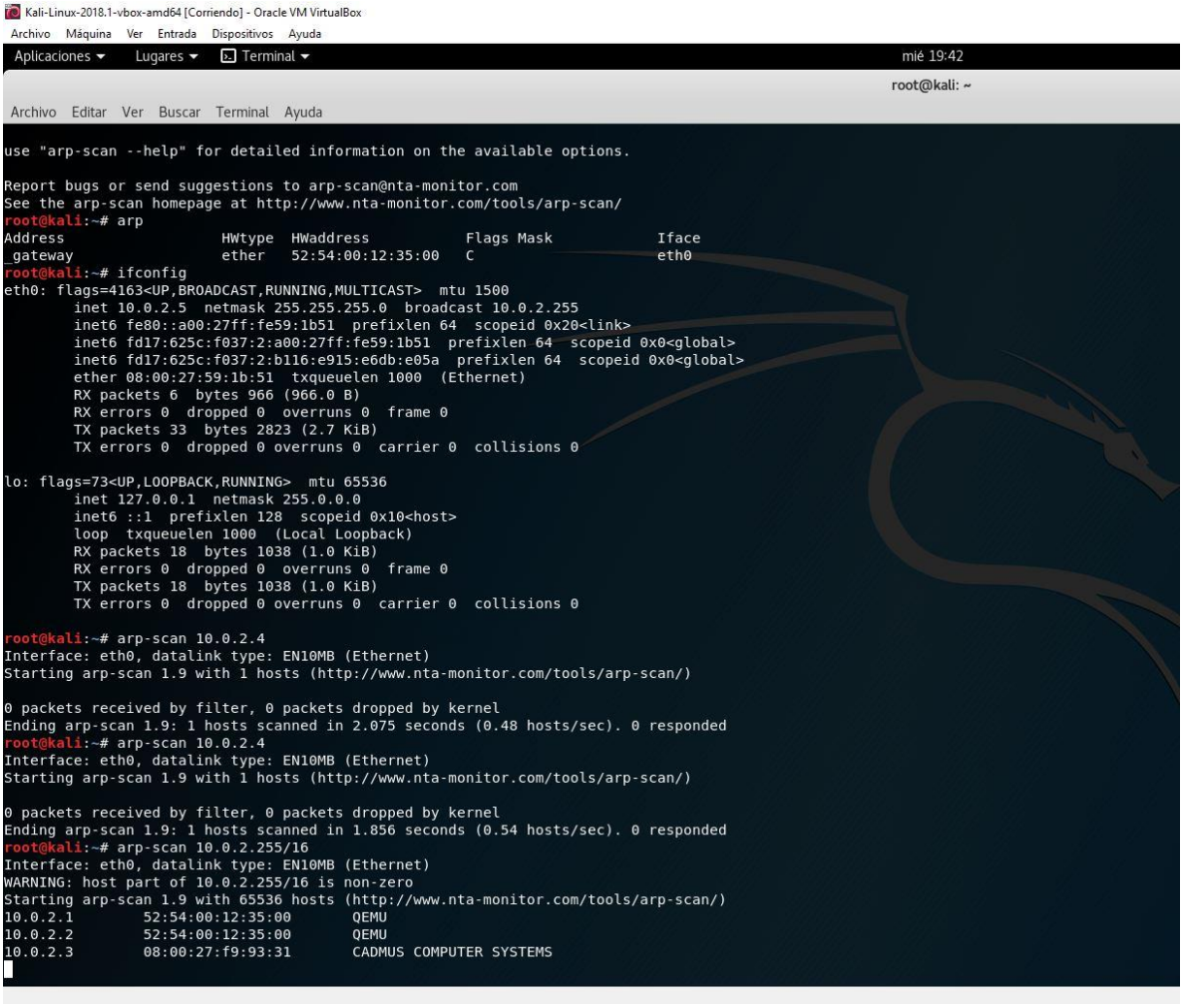
A)


Curso: Seguridad en Sist
SSI - Clase 8 - Presenta
Taller No. 3 - Document
186.0.53.31
Es seguro | https://www.shodan.io/host/186.0.53.31
186.0.53.31 pei-186-0-iiii-xxxi.une.net.co
City Medellin
Country Colombia
Organization UNE
ISP UNE
Last Update 2018-04-30T06:30:58.606230
Hostnames pei-186-0-iiii-xxxi.une.net.co
ASN AS13489
Web Technologies
Google Font API
jQuery
jQuery Migrate
PHP
WordPress
Ports
80
443
Services
80
tcp
http
Apache httpd Version: 2.4.10
HTTP/1.1 301 Moved Permanently
Date: Mon, 30 Apr 2018 06:30:52 GMT
Server: Apache/2.4.10 (Debian)
Set-Cookie: wfvt_1792591643=5ae6b81e4ebfe; expires=Mon, 30-Apr-2018 07:00:54 GMT; Max-Age=1800; path=/; httponly
Set-Cookie: PHPSESSID=6jkrp5rkb7uus90r5iqb3eek40; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: https://www.cotecnova.edu.co/
Content-Length: 0
Content-Type: text/html; charset=UTF-8
443
tcp
https
Apache httpd Version: 2.4.10
HTTP/1.1 200 OK
Date: Mon, 30 Apr 2018 06:30:57 GMT
Server: Apache/2.4.10 (Debian)
Set-Cookie: wfvt_417183207 0=5ae6b82225cb6; expires=Mon, 30-Apr-2018 07:00:58 GMT; Max-Age=1800; path=/; secure; httponly
Set-Cookie: PHPSESSID=m74ft5fatm0jr7939v2utjq870; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Link: <https://www.cotecnova.edu.co/index.php/wp-json/>; rel="https://api.w.org/"
Link: <https://www.cotecnova.edu.co/>; rel=shortlink
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
SSL Certificate
Certificate:
6:26 p. m.
2/05/2018

B)arp –arp scan.

```
Interfaz: 192.168.56.1 --- 0xd
  Dirección de Internet          Dirección física      Tipo
  192.168.56.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.2              01-00-5e-00-00-02     estático
  224.0.0.22             01-00-5e-00-00-16     estático
  224.0.0.251            01-00-5e-00-00-fb     estático
  224.0.0.252            01-00-5e-00-00-fc     estático
  239.255.255.250        01-00-5e-7f-ff-fa     estático

Interfaz: 192.168.2.152 --- 0x12
  Dirección de Internet          Dirección física      Tipo
  192.168.2.1            2e-83-24-64-04-1a     dinámico
  192.168.2.29           f8-0f-41-63-7f-43     dinámico
  192.168.2.66           f8-0f-41-63-7b-de     dinámico
  192.168.2.123          fc-45-96-28-94-42     dinámico
  192.168.2.125          fc-45-96-28-a8-99     dinámico
  192.168.2.131          fc-45-96-28-a8-b0     dinámico
  192.168.2.135          fc-45-96-28-a8-e9     dinámico
  192.168.2.148          f8-0f-41-63-7f-4c     dinámico
  192.168.2.255          ff-ff-ff-ff-ff-ff     estático
  224.0.0.2              01-00-5e-00-00-02     estático
  224.0.0.22             01-00-5e-00-00-16     estático
  224.0.0.251            01-00-5e-00-00-fb     estático
  224.0.0.252            01-00-5e-00-00-fc     estático
  224.0.0.253            01-00-5e-00-00-fd     estático
  239.255.255.250        01-00-5e-7f-ff-fa     estático
  255.255.255.255        ff-ff-ff-ff-ff-ff     estático

C:\Users\SALA E-13>
```

Se muestran todas las redes conecctadas


Kali-Linux-2018.1-vbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Lugares Terminal
mié 19:42
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
use "arp-scan --help" for detailed information on the available options.
Report bugs or send suggestions to arp-scan@nta-monitor.com
See the arp-scan homepage at http://www.nta-monitor.com/tools/arp-scan/
root@kali:~# arp
Address HWtype HWaddress Flags Mask Iface
_gateway ether 52:54:00:12:35:00 C eth0
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.5 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fe59:1b51 prefixlen 64 scopeid 0x20<link>
inet6 fd17:625c:f037:2:a00:27ff:fe59:1b51 prefixlen 64 scopeid 0x0<global>
inet6 fd17:625c:f037:2:b116:e915:e6db:e05a prefixlen 64 scopeid 0x0<global>
ether 08:00:27:59:1b:51 txqueuelen 1000 (Ethernet)
RX packets 6 bytes 966 (966.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 33 bytes 2823 (2.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 18 bytes 1038 (1.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 18 bytes 1038 (1.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~# arp-scan 10.0.2.4
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/arp-scan/)
0 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 1 hosts scanned in 2.075 seconds (0.48 hosts/sec). 0 responded
root@kali:~# arp-scan 10.0.2.4
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/arp-scan/)
0 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 1 hosts scanned in 1.856 seconds (0.54 hosts/sec). 0 responded
root@kali:~# arp-scan 10.0.2.255/16
Interface: eth0, datalink type: EN10MB (Ethernet)
WARNING: host part of 10.0.2.255/16 is non-zero
Starting arp-scan 1.9 with 65536 hosts (http://www.nta-monitor.com/tools/arp-scan/)
10.0.2.1 52:54:00:12:35:00 QEMU
10.0.2.2 52:54:00:12:35:00 QEMU
10.0.2.3 08:00:27:f9:93:31 CADMUS COMPUTER SYSTEMS

c)

```
root@kali:~# nmap
Nmap 7.60 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
```

```
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

```
root@kali:~# nmap 192.168.2.29

Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-02 18:43 -05
Nmap scan report for 192.168.2.29
Host is up (0.0022s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
554/tcp open  rtsp

Nmap done: 1 IP address (1 host up) scanned in 5.05 seconds
```

.

Se realiza un escaneo con la herramienta NMAP done se visualiza los siguientes comportamientos.

D) zenmap

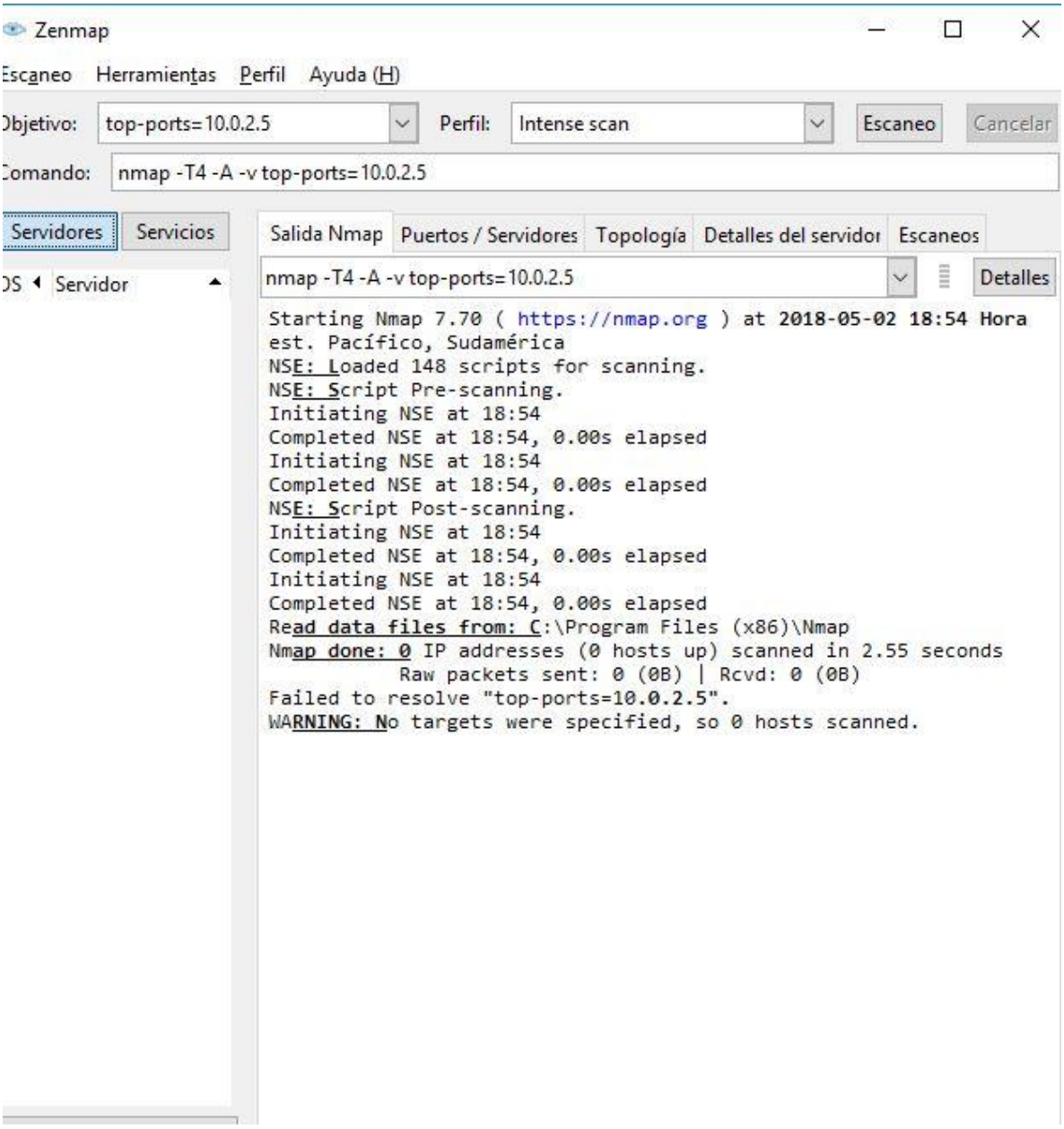


Figure 1Escaneo Zenmap

E) NC

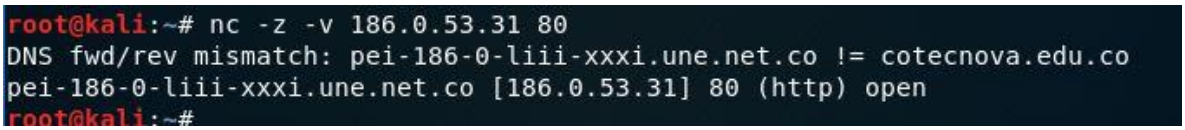
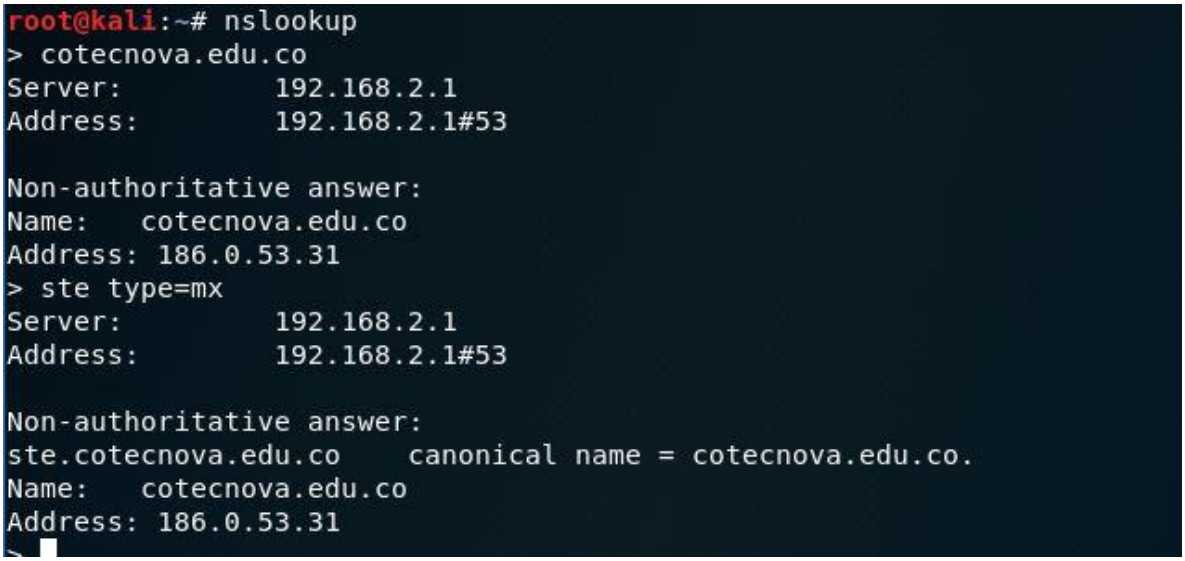


Figure 2Escaneo NC

Escaneo realizado con NC

F) nslookup



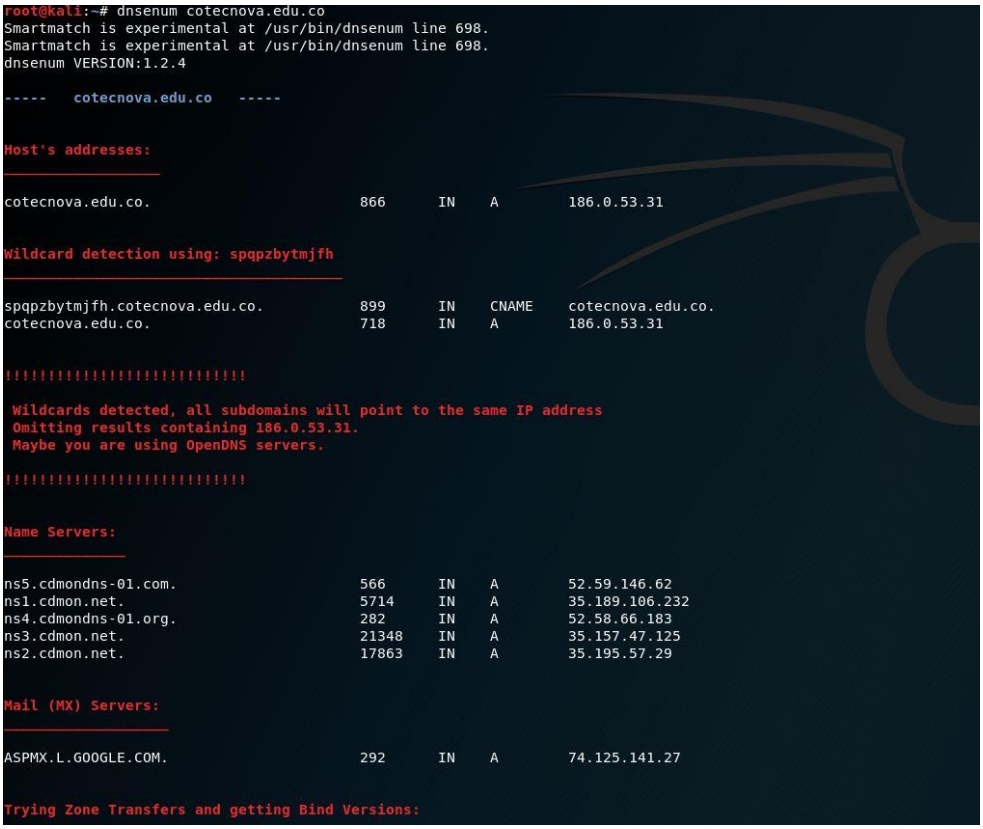
Se escaneo la direccion domino de cotecnova.edu.co con NSLOOKUP

Se observa dirección de servidor. nombre de dominio e IP La pagina

E) dig

```
root@kali:~# dig cotecnova.edu.co

; <<>> DiG 9.11.2-5-Debian <<>> cotecnova.edu.co
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19774
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;cotecnova.edu.co.              IN      A

;; ANSWER SECTION:
cotecnova.edu.co.       536     IN      A       186.0.53.31

;; Query time: 10 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Wed May 02 18:59:49 -05 2018
;; MSG SIZE  rcvd: 50
```

```
root@kali:~# dig dns cotecnova.edu.co

; <<>> DiG 9.11.2-5-Debian <<>> dns cotecnova.edu.co
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58716
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;dns.                           IN      A

;; ANSWER SECTION:
dns.                    0       IN      A       75.125.225.163

;; Query time: 3 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Wed May 02 19:00:34 -05 2018
;; MSG SIZE  rcvd: 37

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3030
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;cotecnova.edu.co.              IN      A

;; ANSWER SECTION:
cotecnova.edu.co.       886     IN      A       186.0.53.31

;; Query time: 1 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Wed May 02 19:00:34 -05 2018
;; MSG SIZE  rcvd: 50
```



Hay varianzas en cuanto a la información que se muestra puesto que en uno muestra el servidor y su IP esto lo hace dig dns

Ambos me muestran las direcciones IP de la universidad

H) Cuadro Comparativo

Whois	Shodan
Es una herramienta muy versátil para la recolección de información importante en un análisis de vulnerabilidades en una red. Puesto que con esta podemos hallar mucha información valiosa de una red. Tal como lo es la información física de la empresa a la cual estamos vulnerando. Sus teléfonos. Dominios, servidores de correo. Con esta herramienta pudimos hallar direcciones físicas, también quien es la persona que realizo la suscrición, que servidor están utilizando, que dominio de correo utilizan. Etc. Esta herramienta da unas características muy detalladas de las redes, siempre y cuando la información no este privatizada. Whois nos sirvió de manera fundamental para hallar información requería en puntos muy específicos del trabajo a realizar. Puesto que al dar información detallada ahorra tiempo al no tener que ir a otros programas para filtrar la información.	Shodan nos da la facilidad de poder ingresar y saber la dirección ip. De donde está ubicado el domino físicamente. Nos brinda también la capacidad de informar cuales son los puertos que están abiertos o funcionando. De manera no privada o cerrada. Deja evidenciar cuales son los servicios que se está corriendo y sus protocolos. Shodan en el proceso de este trabajo fue muy importante para puntos específicos de hallar lugares y dominios que se requerían
Harsvesting	Foca
Como aplicación de filtrado de correos funciona de una muy buena manera puesto que ayuda al filtrado de los correos con un dominio determinado.	Foca como programa de seguimiento de metadatos es una herramienta muy importante para recopilación de información detallada. En muchos de sus aspectos como historiales so raíces. Es un muy buen analizador de archivos y metadatos puesto que con el hacemos penetraciones en archivos y así dictaminando sus vulnerabilidades