

TALLER 3

LUIS CARLOS JORDAN HURTADO

KELLY FERNANDA VÁSQUEZ ZAPATA

JHONATTAN LEANDRO BEDOYA MEJIA

TRABAJO DE:

SEGURIDAD INFORMATICA

PRESENTADO A:

CARLOS ALBERTO LONDOÑO LOAIZA

CARTAGO VALLE

CORPORACIÓN DE ESTUDIOS TECNOLÓGICOS DEL

NORTE DEL VALLE

TECNOLOGIA EN SISTEMAS DE INFORMACIÓN

SEMESTRE V

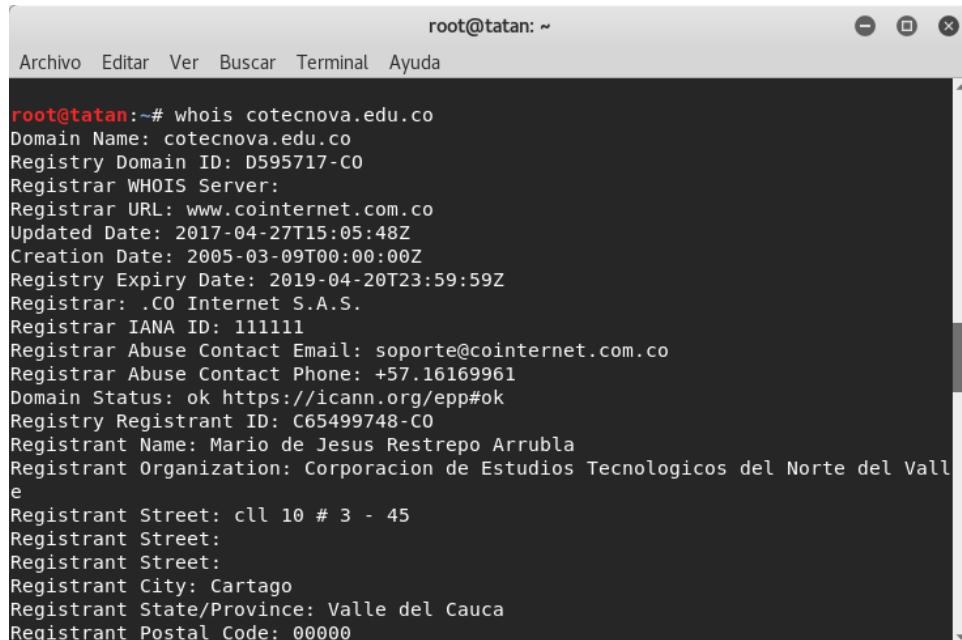
2018

TALLER

1. Obtención de información:

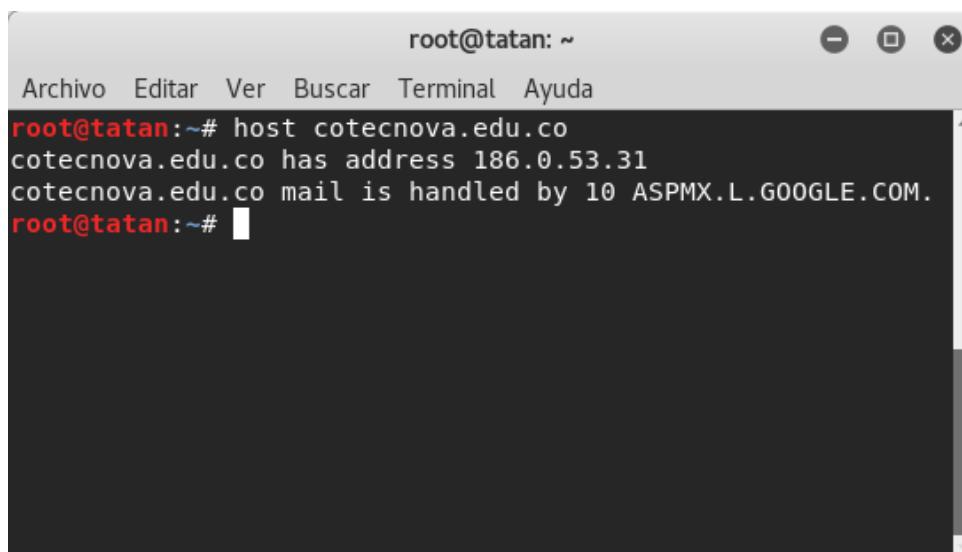
- Usando el protocolo whois, realizar el análisis del dominio

cotecnova.edu.co



```
root@tatan:~# whois cotecnova.edu.co
Domain Name: cotecnova.edu.co
Registry Domain ID: D595717-CO
Registrar WHOIS Server:
Registrar URL: www.cointernet.com.co
Updated Date: 2017-04-27T15:05:48Z
Creation Date: 2005-03-09T00:00:00Z
Registry Expiry Date: 2019-04-20T23:59:59Z
Registrar: .CO Internet S.A.S.
Registrar IANA ID: 11111
Registrar Abuse Contact Email: soporte@cointernet.com.co
Registrar Abuse Contact Phone: +57.16169961
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: C65499748-CO
Registrant Name: Mario de Jesus Restrepo Arrubla
Registrant Organization: Corporacion de Estudios Tecnologicos del Norte del Valle
Registrant Street: cll 10 # 3 - 45
Registrant Street:
Registrant Street:
Registrant City: Cartago
Registrant State/Province: Valle del Cauca
Registrant Postal Code: 00000
```

- Usando el protocolo host, realizar el análisis del dominio cotecnova.edu.co



```
root@tatan:~# host cotecnova.edu.co
cotecnova.edu.co has address 186.0.53.31
cotecnova.edu.co mail is handled by 10 ASPMX.L.GOOGLE.COM.
root@tatan:~#
```

- c. Usando el dominio cotecnova.edu.co usar los siguientes sitios indicando cual es la diferencia de la información que entrega cada una de ellos:

Robtex:

QUICK INFO

cotecnova.edu.co quick info

General	
FQDN	cotecnova.edu.co
Host Name	cotecnova.edu.co
Domain Name	cotecnova.edu.co
Registry	edu.co
TLD	.co

DNS

IP numbers	186.0.53.31
Name servers	ns5.cdmrndns-01.com ns1.cdmmon.net ns2.cdmmon.net ns3.cdmmon.net ns4.cdmrndns-01.org
Mail servers	aspmx.l.google.com

3 Trace IP Address
4 Window Virtual Server
5 SQL Server Database
6 Hide My IP
7 Linux Server Monitoring
8 How to Change IP Address
9 Free IP Address Lookup
10 Change My IP Address

Linux Server Monitoring SMTP Server Change my IP address

This website uses cookies to ensure you get the best experience on our website. [Learn more](#)

ANALYSIS

Cotecnova.edu.co has five name servers, one mail server and one IP number.

Cdmrndns-01 and cdmmon name servers

The name servers are ns5.cdmrndns-01.com, ns1.cdmmon.net, ns2.cdmmon.net, ns3.cdmmon.net and ns4.cdmrndns-01.org.

Google mail server

The mail server is aspmx.l.google.com.

This domain uses google to handle its email.

IP number

The IP number is 186.0.53.31. The PTR of the IP number is pei-186-0-iii-une.net.co. The IP number is in Pereira, Colombia. It is hosted by UNE-ETP.

We investigated two host names that cname to cotecnova.edu.co.

Results found

Cotecnova.tk, cocovagent.com, concovate.com, contacove.com, convocate.com, tacconove.com, tecnocova.com, convocate.info, convocate.net and convocate.nd.edu.

El mejor casino de bitcoin
Gana para ser el Rey
<http://long.com>

1 Apply for Grants Got it!

This website uses cookies to ensure you get the best experience on our website. [Learn more](#)

Ipv4info:

Aplicaciones ▾ Lugares ▾ Firefox ESR ▾ mar 21:34

IPv4Info - 186.0.53.31 ip address information. - Mozilla Firefox

Curso: Seguridad en ... | Taller No. 3 - Docum... | SSI - Clase 8 - Presen... | SSI - Clase 9 - Presen... | IPv4Info - 186.0.53.3... | +

ipv4info.com/ip-address/s6ed5de/186.0.53.31.html/cotecnova.edu.co/#...

Domain **cotecnova.edu.co** is located on IP address <= 186.0.53.31 >=

Block start 186.0.0.0
End of block 186.0.63.255
Block size 16384 Domains in block
Block name
AS number 13489
Parent block 186.0.0.0-186.255.255.255
Organization EMPRESA DE TELECOMUNICACIONES DE PEREIRA S.A.
City Cali
Region/State Valle del Cauca
Country CO - Colombia
Reg. date 2008-06-20
Host name pei-186-0-iii-xci.une.net.co
Web server Apache/2.2.8(CentOS)
Powered by PHP/5.3.29
Domain count >= 13 Servers around

Domains

- 1 [cotecnova.edu.co](#)
- 2 [en.cotecnova.edu.co](#)
- 3 [siyvc.cotecnova.edu.co](#)
- 4 [talentohumano.cotecnova.edu.co](#)
- 5 [www.avaco.cotecnova.edu.co](#)
- 6 [www.biblioteca.cotecnova.edu.co](#)
- 7 [www.catalogo.dg.cotecnova.edu.co](#)
- 8 [www.cotecnova.edu.co](#)
- 9 [www.investigaciones.cotecnova.edu.co](#)

View larger map

Map data ©2018 Google Terms of Use Report a map error

44.78.5.230
akumekmedelminicar.com
185.31.6.80.185.31.6.87
80.74.110.0-80.74.110.31
saltipn.su
valeno.cm
64.210.0.0-64.210.127.255
104.218.84.0-104.218.87.255
197.210.255.0-197.210.255.255
360mail.com
rb.beeline.eu
85.217.10.15
13.3.3.65
offshore.tor
91.80.24.141
workplace.camdata.de
87.150.47.128.82.150.47.191
hq.venkuf.de
104.155.97.187
200.30.1
205.88.186.0-208.68.191.255
space-masters.co.nz

Bgp hurricane:

Aplicaciones ▾ Lugares ▾ Firefox ESR ▾ mar 21:36

cotecnova.edu.co - bgp.he.net - Mozilla Firefox

Curso: Seguridad en ... | Taller No. 3 - Docum... | SSI - Clase 8 - Presen... | SSI - Clase 9 - Presen... | cotecnova.edu.co - ... | +

https://bgp.he.net/dns/cotecnova.edu.co#_ipinfo

HURRICANE ELECTRIC INTERNET SERVICES cotecnova.edu.co Search

Quick Links

- BGP Monitor Home
- BGP Peering 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

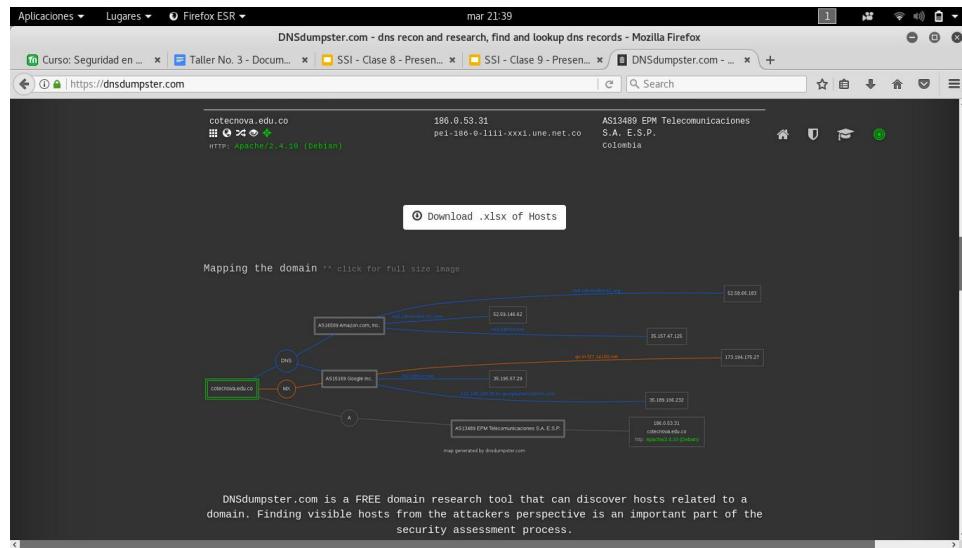
DNS Info | Website Info | IP Info | Whois

186.0.53.31 > 186.0.0.0/17 > AS13489 > EPM Telecommunicaciones S.A. E.S.P.

Updated 24 Apr 2018 16:52 PST © 2018 Hurricane Electric

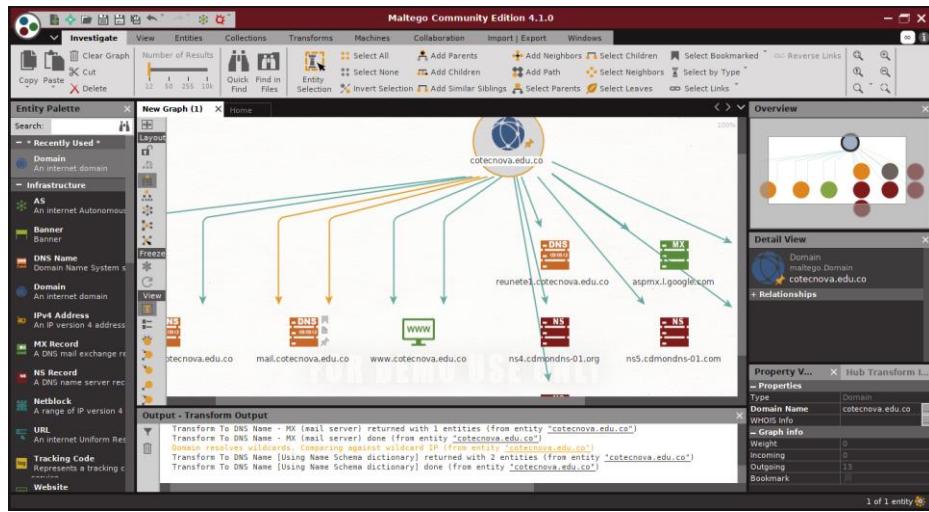
[Twitter](#) [Facebook](#)

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 recon-ng aplicar un módulo que permita obtener información importante del dominio cotecnova.edu.co

```
root@tatan: ~
Archivo Editar Ver Buscar Terminal Ayuda
recon/profiles-contacts/dev_diver
recon/profiles-contacts/github_users
recon/profiles-profiles/namechk
recon/profiles-profiles/profiler
recon/profiles-profiles/twitter_mentioned
recon/profiles-profiles/twitter_mentions
recon/profiles-repositories/github_repos
recon/repositories-profiles/github_commits
recon/repositories-vulnerabilities/gists_search
recon/repositories-vulnerabilities/github_dorks

Reporting
-----
reporting/csv
reporting/html
reporting/json
reporting/list
reporting/proxifier
reporting/pushpin
reporting/xlsx
reporting/xml

[recon-ng][cotecnova.edu.co] > clear
[*] Command: clear

[recon-ng][cotecnova.edu.co] > use recon/domains-vulnerabilities/xssed
[recon-ng][cotecnova.edu.co][xssed] > set SOURCE cotecnova.edu.co
SOURCE => cotecnova.edu.co
[recon-ng][cotecnova.edu.co][xssed] > run

-----
COTECNOVA.EDU.CO
-----
[*] No vulnerabilites found.
[recon-ng][cotecnova.edu.co][xssed] >
```

g. Use theharvester para obtener información adicional a su proceso de investigación del dominio cotecnova.edu.co

```
root@tatan: ~
Archivo Editar Ver Buscar Terminal Ayuda

[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...
    Searching 200 results...
    Searching 300 results...
    Searching 400 results...
    Searching 500 results...

[+] Emails found:
-----
jloaiza@cotecnova.edu.co
rectoriatotecnova@cotecnova.edu.co
cesbarahona@cotecnova.edu.co
convocatoriadocentes@cotecnova.edu.co
carolinaacm@cotecnova.edu.co
frodriguez@cotecnova.edu.co
marlenrm@cotecnova.edu.co
jessicacm@cotecnova.edu.co
sgodoyh@cotecnova.edu.co
wgomez@cotecnova.edu.co
isarojas@cotecnova.edu.co

[+] Hosts found in search engines:
-----
[-] Resolving hostnames IPs...
186.0.53.31:Biblioteca.cotecnova.edu.co
186.0.53.31:avaco.cotecnova.edu.co
186.0.53.31:biblioteca.cotecnova.edu.co
186.0.53.31:investigaciones.cotecnova.edu.co
186.0.53.31:www.avaco.cotecnova.edu.co
186.0.53.31:www.biblioteca.cotecnova.edu.co
186.0.53.31:www.cotecnova.edu.co
186.0.53.31:www.recibo.cotecnova.edu.co
root@tatan: ~#
```

- 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 archivos del dominio cotecnova.edu.co

Id	Type	URL	Download	Download Date	Size	Analyzed	Modified Date
1	pdf	http://www.recko.cotecnova.edu.co/INSTRUCTIVO_G...	x	-	622.23 KB	x	-
2	pdf	http://www.cotecnova.edu.co/wp-content/uploads/201...	x	-	68.61 KB	x	-
3	pdf	http://www.cotecnova.edu.co/wp-content/uploads/201...	x	-	68.26 KB	x	-
4	pdf	http://www.recko.cotecnova.edu.co/fpdocs/pdf/	x	-	27.11 KB	x	-
5	pdf	http://www.cotecnova.edu.co/wp-content/uploads/201...	x	-	421.24 KB	x	-
6	pdf	http://www.cotecnova.edu.co/wp-content/uploads/201...	x	-	1.53 MB	x	-
7	pdf	http://www.cotecnova.edu.co/wp-content/uploads/201...	x	-	715.92 KB	x	-
8	pdf	http://www.cotecnova.edu.co/wp-content/uploads/201...	x	-	203.91 KB	x	-
	pdf	http://www.cotecnova.edu.co/wp-content/uploads/2011...	v	-	2.74 MB	v	-

- j. Resuma en un cuadro comparativo la información más importante que considere obtuvo de este proceso que le servirá para una auditoría y con qué herramienta la obtuvo.

k.

HERRAMIENTA	DESCRIPCIÓN
WHOIS	Con esta utilidad, podremos analizar la información pública del dominio, tal como lo son los registros de este en otros servidores DNS de la red.
BROWSER HACKING	Herramienta utilizada para realizar búsquedas del servidor , ya que puedes que exista algún tipo de vulnerabilidad que no se pueda evidenciar en otro aplicativo.
ROPTEX	Esta herramienta, complementa un poco mas frente a la información suministrada por parte de whois.
HARVESTER	Este aplicativo nos ayuda a explorar que tipo de vulnerabilidad podemos hallar en el dominio frente a sus limitantes con la pagina, correo entre otros.
FOCA	Realizando uso de este software podemos realizar un scaneo a determinado dominio, en el cual podremos visualizar si existe algún tipo de documento o archivo que nos pueda ser de utilidad.

2. Enumeración de Sistemas:

- Consultar en shodan la información que pueda obtener del dominio

cotecnova.edu.co

186.0.53.31 pei-186-0-iii-xxxi.une.net.co

Ports

21	80	445
----	----	-----

Services

21	220 Bienvenido Server Desarrollo (Pbas) Cotecnova.
80	530 Permission denied.
445	530 Please login with USER and PASS.

Apache httpd Version: 2.4.10

Aplicaciones ▾ Lugares ▾ Firefox ESR ▾ mar 22:32

cotecnova - Shodan Search - Mozilla Firefox

186.0.53.31

TOP RESULTS

1

TOP COUNTRIES

Colombia 1

TOP ORGANIZATIONS

Empresa De Telecomunicaci... 1

186.0.53.31

220 Bienvenido Server Desarrollo (Pbas) **Cotecnova**.

530 Permission denied.

530 Please login with USER and PASS.

211-Features:

EPGV
EPSV
MDTM
PASV
REST STREAM
SIZE
TVFS
211 End

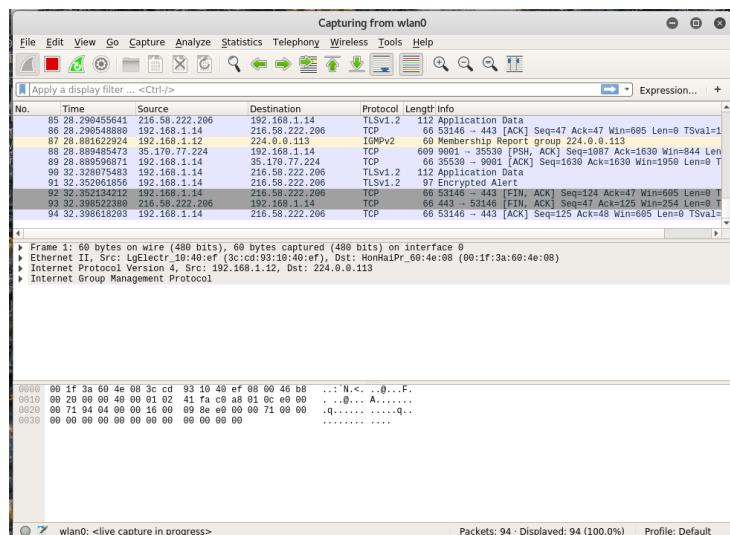
- Realice un escaneo usando arp, arp-scan, wireshark

```
luisjordan@kalinetlc:~$ sudo arp-scan 192.168.1.0/24
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.1.1      a0:f3:c1:96:46:24      TP-LINK TECHNOLOGIES CO., LTD.
192.168.1.105    d0:50:99:57:8d:5a      ASRock Incorporation
192.168.1.100    94:35:0a:16:1b:24      Samsung Electronics Co.,Ltd
192.168.1.101    28:27:bf:50:fa:a5      (Unknown)
192.168.1.102    dc:44:b6:f1:c4:33      (Unknown)
192.168.1.103    f8:3f:51:92:bd:69      (Unknown)
192.168.1.107    84:98:66:a4:33:8d      (Unknown)

7 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.735 seconds (93.60 hosts/sec). 7 responded
luisjordan@kalinetlc:~$ sudo arp
Address          HWtype  HWaddress            Flags Mask           Iface
_gateway         ether    a0:f3:c1:96:46:24  C               eth0
_gateway         ether    a0:f3:c1:96:46:24  C               wlan0
luisjordan@kalinetlc:~$ sudo arp -n
Address          HWtype  HWaddress            Flags Mask           Iface
192.168.1.1      ether    a0:f3:c1:96:46:24  C               eth0
192.168.1.1      ether    a0:f3:c1:96:46:24  C               wlan0
luisjordan@kalinetlc:~$ sudo arp -a 192.168.1.105
arp: in 2 entries no match found.
luisjordan@kalinetlc:~$ sudo arp -i eth0
Address          HWtype  HWaddress            Flags Mask           Iface
_gateway         ether    a0:f3:c1:96:46:24  C               eth0
luisjordan@kalinetlc:~$ sudo arp -i wlan0
Address          HWtype  HWaddress            Flags Mask           Iface
_gateway         ether    a0:f3:c1:96:46:24  C               wlan0
luisjordan@kalinetlc:~$ 
```

```
luisjordan@kalinetlcj: ~
Archivo Editar Ver Buscar Terminal Ayuda
luisjordan@kalinetlcj:~$ sudo arp-scan 192.168.1.0/24
[sudo] password for luisjordan:
Interface: wlan0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/
)
192.168.1.12  3c:cd:93:10:40:ef      (Unknown)
192.168.1.16  d0:fc:cc:c4:cb:c7      (Unknown)
192.168.1.15  24:da:9b:f4:33:61      (Unknown)
192.168.1.17  f0:03:8c:42:61:eb      (Unknown)
192.168.1.22  4c:bb:58:ef:93:0e      (Unknown)
192.168.1.29  f0:03:8c:42:61:eb      (Unknown)
192.168.1.11  2c:fd:a1:d7:88:45      (Unknown)
192.168.1.254 ac:20:2e:e7:e5:32      (Unknown)

8 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 3.308 seconds (77.39 hosts/sec). 8 res-
ponded
luisjordan@kalinetlcj:~$
```



- c. Realizar un escaneo profundo de la red usando la herramienta nmap que permita obtener información importante

```
luisjordan@kalinetlcj:~  
Archivo Editar Ver Buscar Terminal Ayuda  
  
luisjordan@kalinetlcj:~$ sudo nmap cotecnova.edu.co  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-29 10:44 -05  
Nmap scan report for cotecnova.edu.co (186.0.53.31)  
Host is up (0.020s latency).  
rDNS record for 186.0.53.31: pei-186-0-liii-xxxi.une.net.co  
Not shown: 995 filtered ports  
PORT      STATE SERVICE  
20/tcp    closed  ftp-data  
21/tcp    open   ftp  
80/tcp    open   http  
443/tcp   open   https  
9000/tcp  open   cslistener  
  
Nmap done: 1 IP address (1 host up) scanned in 10.56 seconds  
luisjordan@kalinetlcj:~$ sudo nmap -Ss cotecnova.edu.co  
WARNING: If -S is being used to fake your source address, you may also have to use -e <inteface> and -Pn . If you are using it to specify your real source address, you can ignore t his warning.  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-29 10:45 -05  
Could not figure out what device to send the packet out on with the source address you gave  
me! If you are trying to spoof your scan, this is normal, just give the -e eth0 or -e ppp  
0 or whatever. Otherwise you can still use -e, but I find it kind of fishy.  
QUITTING!  
luisjordan@kalinetlcj:~$ sudo nmap -Ss cotecnova.edu.co  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-29 10:46 -05  
Nmap scan report for cotecnova.edu.co (186.0.53.31)  
Host is up (0.067s latency).  
rDNS record for 186.0.53.31: pei-186-0-liii-xxxi.une.net.co  
Not shown: 995 filtered ports  
PORT      STATE SERVICE  
20/tcp    closed  ftp-data  
21/tcp    open   ftp  
80/tcp    open   http  
443/tcp   open   https  
9000/tcp  open   cslistener  
  
Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds  
luisjordan@kalinetlcj:~$ sudo nmap -ST cotecnova.edu.co  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-29 10:46 -05
```

```
luisjordan@kalinetlcj: ~
Archivo Editar Ver Buscar Terminal Ayuda

Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
luisjordan@kalinetlcj:~$ sudo nmap -sT cotechnova.edu.co
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-29 10:46 -05
Nmap scan report for cotechnova.edu.co (186.0.53.31)
Host is up (0.019s latency).
rDNS record for 186.0.53.31: pe1-186-0-lili1-xxxi.une.net.co
Not shown: 996 filtered ports
PORT      STATE SERVICE
20/tcp    closed  ftp-data
21/tcp    open   ftp
80/tcp    open   http
9000/tcp  open   cslistener

Nmap done: 1 IP address (1 host up) scanned in 12.95 seconds
luisjordan@kalinetlcj:~$ sudo nmap -b cotechnova.edu.co
Hint: if your bounce scan target hosts aren't reachable from here, remember to use -Pn so we don't try and ping them prior to the scan
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-29 10:47 -05
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.27 seconds
luisjordan@kalinetlcj:~$ sudo nmap -sT -b -n -vv cotechnova.edu.co
Hint: if your bounce scan target hosts aren't reachable from here, remember to use -Pn so we don't try and ping them prior to the scan
You specified more than one type of TCP scan. Please choose only one of -sA, -b, -sT, -sF, -sI, -sM, -sN, -sS, -sW, and -sX
QUITTING!
luisjordan@kalinetlcj:~$ sudo nmap -sT -n -vv cotechnova.edu.co
Starting Nmap 7.70 ( https://nmap.org ) at 2018-04-29 10:48 -05
Initiating Ping Scan at 10:48
Scanning cotechnova.edu.co (186.0.53.31) [4 ports]
Completed Ping Scan at 10:49, 0.04s elapsed (1 total hosts)
Initiating Connect Scan at 10:48
Scanning cotechnova.edu.co (186.0.53.31) [1000 ports]
Discovered open port 21/tcp on 186.0.53.31
Discovered open port 443/tcp on 186.0.53.31
Discovered open port 80/tcp on 186.0.53.31
Discovered open port 9000/tcp on 186.0.53.31
Completed Connect Scan at 10:48, 4.76s elapsed (1000 total ports)
Nmap scan report for cotechnova.edu.co (186.0.53.31)
```

```
luisjordan@kalinetlcj: ~
Archivo Editar Ver Buscar Terminal Ayuda
Discovered open port 443/tcp on 186.0.53.31
Discovered open port 80/tcp on 186.0.53.31
Discovered open port 9000/tcp on 186.0.53.31
Completed Connect Scan at 10:48, 4.76s elapsed (1000 total ports)
Nmap scan report for cotecnova.edu.co (186.0.53.31)
Host is up, received echo-reply ttl 57 (0.028s latency).
Scanned at 2018-04-29 10:48:21 -05 for 5s
Not shown: 995 filtered ports
Reason: 995 no-responses
PORT      STATE SERVICE      REASON
20/tcp    closed  ftp-data   conn-refused
21/tcp    open   ftp          syn-ack
80/tcp    open   http         syn-ack
443/tcp   open   https        syn-ack
9000/tcp  open   cslistener  syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.15 seconds
  Raw packets sent: 4 (152B) | Rcvd: 1 (28B)
luisjordan@kalinetlcj: $ sudo nmap -P0 -sU -n -vv cotecnova.edu.co
Warning: The -P0 option is deprecated. Please use -Pn
Starting Nmap 7.00 ( https://nmap.org ) at 2018-04-29 10:50
Initiating UDP Scan at 10:50
Scanning cotecnova.edu.co (186.0.53.31) [1000 ports]
  UDP Scan Timing: About 15.50% done; ETC: 10:53 (0:02:49 remaining)
  UDP Scan Timing: About 30.50% done; ETC: 10:53 (0:02:19 remaining)
  UDP Scan Timing: About 45.50% done; ETC: 10:53 (0:01:49 remaining)
  UDP Scan Timing: About 60.50% done; ETC: 10:53 (0:01:19 remaining)
  UDP Scan Timing: About 75.50% done; ETC: 10:53 (0:00:49 remaining)
Completed UDP Scan at 10:53, 201.28s elapsed (1000 total ports)
Nmap scan report for cotecnova.edu.co (186.0.53.31)
Host is up, received user-set.
All 1000 scanned ports on cotecnova.edu.co (186.0.53.31) are open|filtered because of 1000
no-responses

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 206.58 seconds
  Raw packets sent: 2000 (57.854KB) | Rcvd: 0 (0B)
luisjordan@kalinetlcj: $
```

```
luisjordan@kalinetlcj:~
```

Archivo Editar Ver Buscar Terminal Ayuda

luisjordan@kalinetlcj:\$ sudo nmap -P0 -sT -O -n -vv cotecnova.edu.co

Warning: The -P0 option is deprecated. Please use -Pn

Starting Nmap 7.70 (https://nmap.org) at 2018-04-29 10:57 -05

Initiating Connect Scan at 10:58

Scanning cotecnova.edu.co (186.0.53.31) [1000 ports]

Discovered open port 443/tcp on 186.0.53.31

Discovered open port 80/tcp on 186.0.53.31

Discovered open port 21/tcp on 186.0.53.31

Discovered open port 9000/tcp on 186.0.53.31

Completed Connect Scan at 10:58, 9.75s elapsed (1000 total ports)

Initiating OS detection (try #1) against cotecnova.edu.co (186.0.53.31)

Retrying OS detection (try #2) against cotecnova.edu.co (186.0.53.31)

Nmap scan report for cotecnova.edu.co (186.0.53.31)

Host is up, received user-set (0.036s latency).

Scanned at 2018-04-29 10:58:00 -05 for 14s

Not shown: 995 filtered ports

Reason: 995 no-responses

PORT	STATE	SERVICE	REASON
20/tcp	closed	ftp-data	conn-refused
21/tcp	open	ftp	syn-ack
80/tcp	open	http	syn-ack
443/tcp	open	https	syn-ack
9000/tcp	open	cslistener	syn-ack

Device type: general purpose|WAP|specialized|storage-misc|broadband router|printer

Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (94%), Asus embedded (90%), Crestron 2-Series (89%), HP embedded (89%)

OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:cpe:/h:asus:rt-ac66u cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3 cpe:/o:linux:linux_kernel:3.4 cpe:/o:linux:linux_kernel:2.6.22

OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU

Aggressive OS guesses: Linux 3.10 - 4.11 (94%), Linux 3.13 (94%), Linux 3.13 or 4.2 (94%), Linux 4.2 (94%), Linux 4.4 (94%), Linux 3.16 (92%), Linux 3.16 - 4.6 (92%), Linux 3.12 (91%), Linux 3.2 - 4.9 (91%), Linux 3.8 - 3.11 (91%)

No exact OS matches for host (test conditions non-ideal).

TCP/IP fingerprint:

SCAN[V=7.70,E=4%D=4%/29%OT=21%CT=20%CU=4%PV=N%G=N%TM=5A5E8B97%P=x86_64-pc-linux-gnu)
SEQ[S=106%GCD=1%ISR=10C%T=Z%CI=I%II=I%TS=8]
OPS[01=M5A0ST11NW6%02=M5A0ST11NW6%03=M5A0NN11NW6%04=M5A0ST11NW6%05=M5A0ST11NW6%06=M5A0ST11
WTN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120%)

```

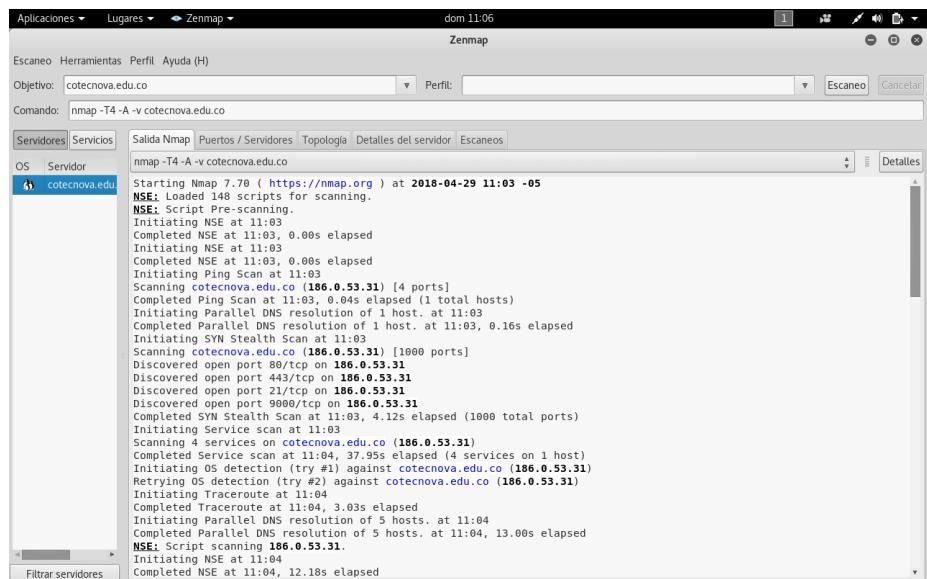
luisjordan@kalineticj: ~
Archivo Editar Ver Buscar Terminal Ayuda
443/tcp open https syn-ack
9000/tcp open cslistener syn-ack Monitor del
Device type: general purpose|WAP|specialized|storage-misc|broadband router|printer
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (94%), Asus embedded (90%), Crestron 2-Series
(89%), HP embedded (89%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:c
pe:/h:asus:rt-ac66u cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3 cpe:/o:linux:linux_kernel:3
.4 cpe:/o:linux:linux_kernel:2.6.22
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
Aggressive OS guesses: Linux 3.10 - 4.11 (94%), Linux 3.13 (94%), Linux 3.13 or 4.2 (94%),
Linux 4.2 (94%), Linux 4.4 (94%), Linux 3.16 (92%), Linux 3.16 - 4.6 (92%), Linux 3.12 (91%),
Linux 3.2 - 4.9 (91%), Linux 3.8 - 3.11 (91%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.70%E=4%D=4/29%T=21%CT=20%C=U=PV=N%G=N%TM=5AE5EB97%P=x86_64-pc-linux-gnu)
SEQ(SP=106%GC=1%ISR=10C%TI=2%C=I=I%I=S=8)
OPS(OI=M5A0ST11NW6%O2=M5A0ST11NW6%O3=M5A0NT11NW6%O4=M5A0ST11NW6%O5=M5A0ST11NW6%O6=M5A0ST11
)
WIN(WI=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)
ECN(R=Y%DF=Y%TG=40%W=0%A=S+%F=AS%RD=0%Q=)
T1(R=Y%DF=Y%TG=40%W=0%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)
T5(R=Y%DF=Y%TG=40%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)
T6(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)
T7(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=40%CD=S)

Uptime guess: 9.012 days (since Fri Apr 20 10:40:55 2018)
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 20.41 seconds
    Raw packets sent: 60 (6.108KB) | Rcvd: 28 (1.932KB)
luisjordan@kalineticj:~$ 

```

- d. Realizar un escaneo profundo de la red usando la herramienta zenmap que permita obtener información importante



Aplicaciones ▾ Lugares ▾ Zenmap ▾

dom 11/06

Zenmap

Escaneo Herramientas Perfil Ayuda (H)

Objetivo: **cotecnova.edu.co**

Perfil:

Comando: nmap -T4 -A -v cotecnova.edu.co

Escaneo Cancelar

Servidores Servicios

OS Servidor

cotecnova.edu.co

Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos

nmap -T4 -A -v cotecnova.edu.co

INITIALIZING NSE at 11:04

Completed NSE at 11:04. 0.06s elapsed

Nmap scan report for **cotecnova.edu.co** (**186.0.53.31**)

Host is up (0.049s latency).

rDNS record for **186.0.53.31**: **pel-186-0-l1ii-xxi.une.net.co**

Not shown: 995 filtered ports

PORT	STATE	SERVICE	VERSION
20/tcp	closed	ftp-data	
21/tcp	open	ftp	vsftpd 2.0.8 or later
80/tcp	open	http	Apache httpd 2.4.10 ((Debian))
		http-cookie-flags:	
	/	PHPSESSID:	
		httponly flag not set	
		http-methods:	
		Supported Methods: GET HEAD POST OPTIONS	
		http-server-header: Apache/2.4.10 (Debian)	
		http-title: Did not follow redirect to https://www.cotecnova.edu.co/	
443/tcp	open	ssl/ssl	Apache httpd (SSL-only mode)
		http-cookie-flags:	
	/	PHPSESSID:	
		httponly flag not set	
		http-methods:	
		Supported Methods: GET HEAD POST OPTIONS	
		http-server-header: Apache/2.4.10 (Debian)	
		http-title: Did not follow redirect to https://www.cotecnova.edu.co/	
		ssl-cert: Subject: commonName=www.cotecnova.edu.co	
		Subject Alternative Name: DNS:www.cotecnova.edu.co	
		Issuer: commonName=Let's Encrypt Authority X3/organizationName=Let's Encrypt/countryName=US	
		Public Key type: rsa	

The screenshot shows the Zenmap interface with the following details:

- Aplicaciones ▾**, **Lugares ▾**, **Zenmap ▾** in the top-left.
- dom 11:06** in the top-right.
- Zenmap** title bar.
- Escaneo Herramientas Perfil Ayuda (H)** menu bar.
- Objetivo:** `cotenova.edu.co`
- Comando:** `nmap -T4 -A -v cotenova.edu.co`
- Perfil:** dropdown menu.
- Escaneo** and **Cancilar** buttons.
- Servidores Servicios** tabs selected.
- Salida Nmap** tab selected.
- Puertos / Servidores**, **Topología**, **Detalles del servidor**, **Escaneos** tabs.
- OS Servidor**:
 - cotenova.edu.co** entry with a blue icon.
 - Device type:** general purpose|WAP|specialized|storage-misc|broadband router|printer
 - Running (JUST GUESSING):** Linux 3.X|4.X|2.X (94%), Asus embedded (90%), Crestech 2-Series (89%), HP embedded (89%)
 - OS CPE:** cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:haswell-ac66u:cpe:/o:restek:restek_3000_g3:cpe:/o:restek:restek_kernel:2.6.22 cpe:/o:linux:linux_kernel:2.6
 - Available OS guesses:** Linux 3.16 (94%), Linux 3.16 - 4.11 (94%), Linux 3.13 (94%), Linux 3.13 or 4.2 (94%), Linux 4.2 (94%), Linux 4.4 (94%), Linux 3.16 (92%), Linux 3.16 - 4.6 (92%), Linux 3.12 (91%), Linux 3.18 (91%), Linux 3.2 - 4.9 (91%)
 - No exact OS matches found for host (test conditions non-ideal).**
 - Uptime guess:** 8.870 days (since Fri Apr 20 14:11:20 2018)
 - Network Distance:** 7 hops
 - TCP Sequence Prediction:** Difficulty=260 (Good luck!)
 - IP ID Sequence Generation:** All zeros
- TRACEROUTE** (using port 20/tcp)

HOP	RTT	ADDRESS
1	0.68 ms	192.168.1.1
2	1.71 ms	192.168.0.1
3	2.44 ms	192.168.2.1
4	14.69 ms	172.16.1.1
5	... 6	
7	77.78 ms	pei-186-0-liii-xxxi.une.net.co (186.0.53.31)
- NSE:** Script Post-scanning.
 - Initiating NSE at 11:04
 - Completed NSE at 11:04, 0.00s elapsed
 - Initiating NSE at 11:04
 - Completed NSE at 11:04, 0.00s elapsed
- Read data files from:** /usr/bin/../share/nmap
- OS and Service detection performed.** Please report any incorrect results at <https://nmap.org/submit/>.
- Nmap done:** 1 IP address (host up) scanned in 82.77 seconds
 - Raw packets sent: 2074 (94.65KB) | Rcvd: 41 (2.504KB)

Aplicaciones ▾ Lugares ▾ Zenmap ▾ dom 11:13

Zenmap

Escaneo Herramientas Perfil Ayuda (H)

Objetivo: cotecnova.edu.co

Perfil: Escaneo Cancelar

Comando: nmap -sT -sU -O -v -n -Pn cotecnova.edu.co

Servidores Servicios

OS Servidor

cotecnova.edu

Starting Nmap 7.70 (https://nmap.org) at 2018-04-29 11:07 -05

Initiating UDP Scan at 11:08

Scanning cotecnova.edu.co (186.0.53.31) [1000 ports]

UDP Scan Timing: About 15.00% done; ETC: 11:11 (0:02:56 remaining)

UDP Scan Timing: About 30.00% done; ETC: 11:11 (0:02:22 remaining)

UDP Scan Timing: About 44.95% done; ETC: 11:11 (0:01:51 remaining)

UDP Scan Timing: About 59.95% done; ETC: 11:11 (0:01:21 remaining)

UDP Scan Timing: About 74.95% done; ETC: 11:11 (0:00:50 remaining)

Completed UDP Scan at 11:11, 201.28s elapsed (1000 total ports)

Initiating Connect Scan at 11:11, 4.76s elapsed (1000 total ports)

Scanning cotecnova.edu.co (186.0.53.31) [1000 ports]

Discovered open port 86/tcp on 186.0.53.31

Discovered open port 21/tcp on 186.0.53.31

Discovered open port 443/tcp on 186.0.53.31

Discovered open port 9000/tcp on 186.0.53.31

Completed Connect Scan at 11:11, 4.76s elapsed (1000 total ports)

Initiating OS detection (try #1) against cotecnova.edu.co (186.0.53.31)

Retrying OS detection (try #2) against cotecnova.edu.co (186.0.53.31)

Retrying OS detection (try #3) against cotecnova.edu.co (186.0.53.31)

Retrying OS detection (try #4) against cotecnova.edu.co (186.0.53.31)

Retrying OS detection (try #5) against cotecnova.edu.co (186.0.53.31)

Nmap scan results for cotecnova.edu.co (186.0.53.31)

Host is up (received user-set 0.12s latency).

Scanned at 2018-04-29 11:08:01 -05 for 219s

Net shome: 1000 open/filtered ports, 995 filtered ports

Reason: 1995 no-responses

PORT	STATE	SERVICE	REASON
20/tcp	closed	ftp-data	conn-refused
21/tcp	open	ftp	syn-ack
80/tcp	open	http	syn-ack
443/tcp	open	https	syn-ack
9000/tcp	open	cslistener	syn-ack

Filtrar servidores

Aplicaciones ▾ Lugares ▾ Zenmap ▾ dom 11:13

Zenmap

Escaneo Herramientas Perfil Ayuda (H)

Objetivo: cotecnova.edu.co

Perfil: Escaneo Cancelar

Comando: nmap -sT -sU -O -v -n -Pn cotecnova.edu.co

Servidores Servicios

OS Servidor

cotecnova.edu

Nmap scan report for cotecnova.edu.co (186.0.53.31)

Host is up (Received user-set 0.12s latency).

Scanned at 2018-04-29 11:08:01 -05 for 219s

Net shome: 1000 open/filtered ports, 995 filtered ports

Reason: 1995 no-responses

PORT	STATE	SERVICE	REASON
20/tcp	closed	ftp-data	conn-refused
21/tcp	open	ftp	syn-ack
80/tcp	open	http	syn-ack
443/tcp	open	https	syn-ack
9000/tcp	open	cslistener	syn-ack

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).

TCP/IP fingerprint:

```

OS:SCAN(V=7.70 O=TCP T=2980 T=211C T=298 CUP=PV=NG=YTM=5AE5EBD%P=886 G4=PC-
OS:25=40D=5A0ST11NW0=02=MSA0NT11NW0%05=MSA0ST11NW0%06=MSA0ST1
OS:40D=2=MSA0ST11NW0=02=MSA0NT11NW0%04=MSA0ST11NW0%05=MSA0ST11NW0%06=MSA0ST1
OS:40D=2=MSA0ST11NW0=02=MSA0NT11NW0%04=MSA0ST11NW0%05=MSA0ST11NW0%06=MSA0ST1
OS:1)WIN(W=7120W=W=7120W=W=7120W=W=7120W=W=7120W=ECDN(R=YSDF=Y3TG=49
OS:W=7210%0=MSA0NNSHW%0=C=Y0=0=TT1(R=YSDF=Y3TG=40%0=A=5%F=AS5RD=0%Q=)T2(
OS:R=N)T3(R=N)T4(R=YDF=Y%G=40W=0%A=Z%F=R%0=RD=0%Q=)T5(R=YDF=Y%G=4
OS:0%W=0%Z=0%A=5%F=AR0=0%RD=0%Q=)T6(R=YDF=Y%G=40%W=0%A=Z%F=R%0=RD=0
OS:0%Q=)T7(R=N)U1(R=N)IE(R=YDFI=NSTG=40%CD=5)

```

Uptime guess: 8.698 days (since Fri Apr 20 18:26:17 2018)

TCP Sequence Prediction: Difficulty=254 (Good luck!)

IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 224.71 seconds

Raw packets sent: 2141 (72.624KB) | Rcvd: 60 (4.270KB)

Filtrar servidores

Aplicaciones ▾ Lugares ▾ Zenmap ▾ dom 11:13

Zenmap

Escaneo Herramientas Perfil Ayuda (H)

Objetivo: cotecnova.edu.co

Perfil: Escaneo Cancelar

Comando: nmap -sT -sU -O -v -n -Pn cotecnova.edu.co

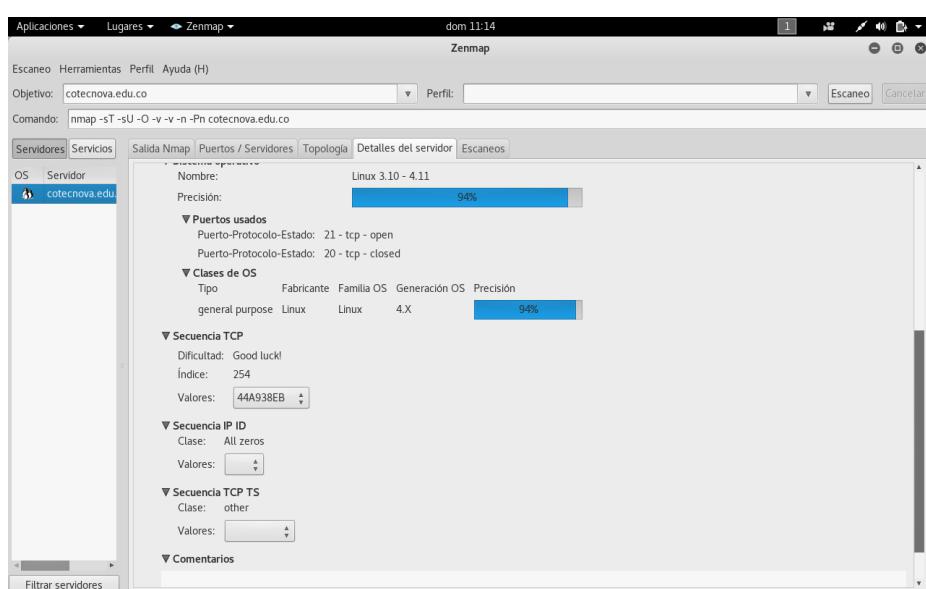
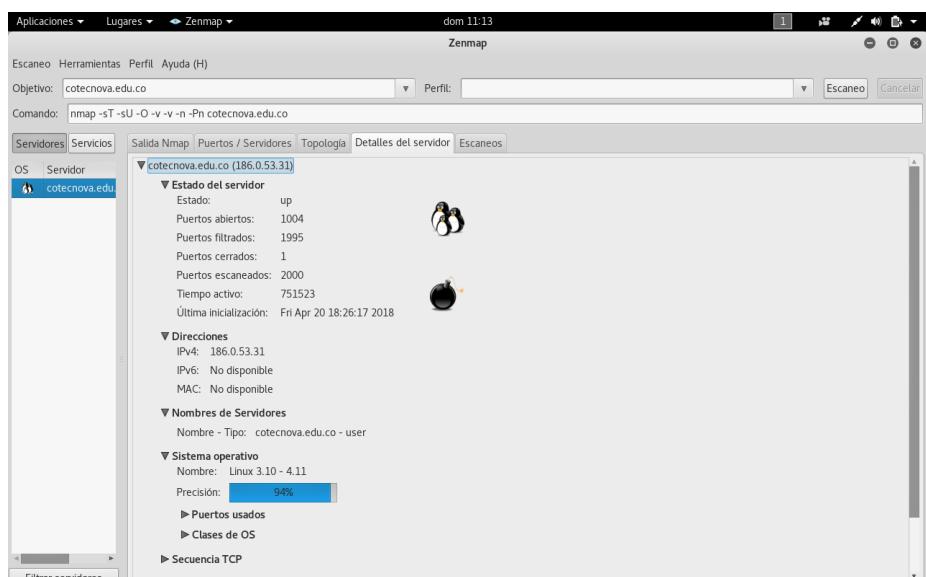
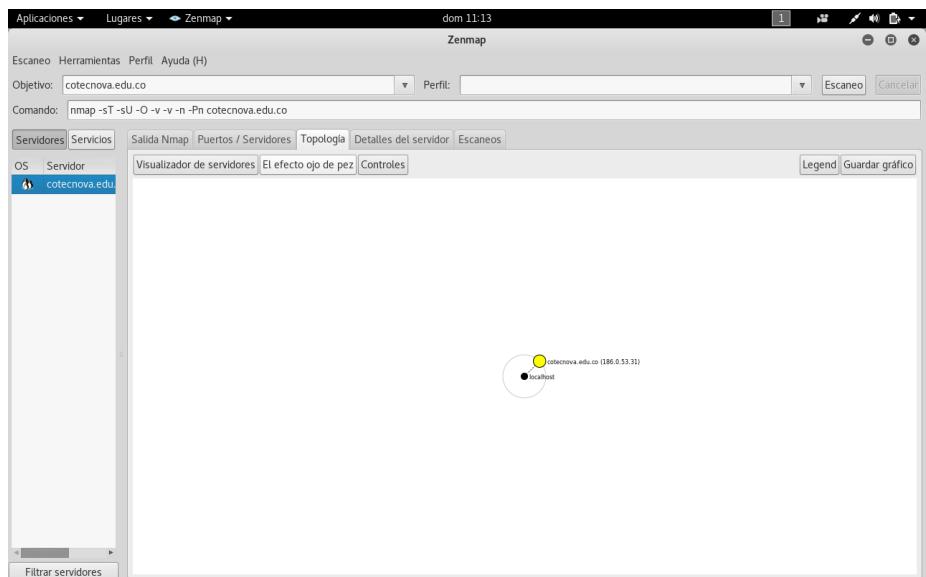
Servidores Servicios

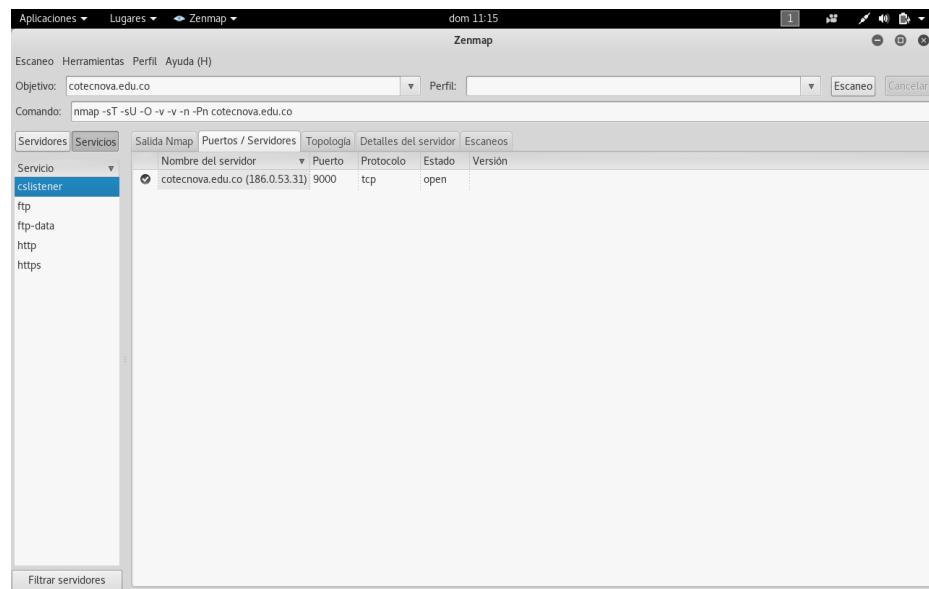
OS Servidor

cotecnova.edu

Puerto	Protocolo	Estado	Servicio	Versión
20	tcp	closed	ftp-data	
21	tcp	open	ftp	
80	tcp	open	http	
443	tcp	open	https	
9000	tcp	open	cslistener	

Filtrar servidores

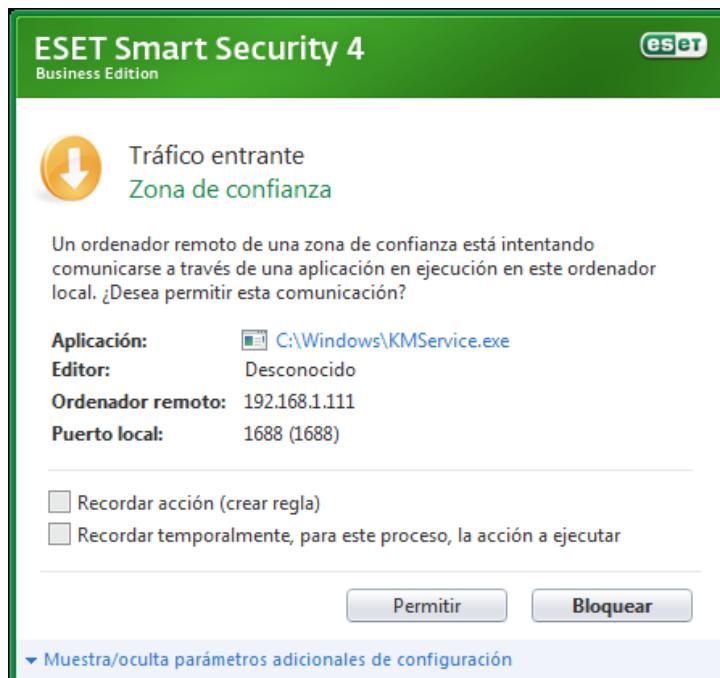




e. Escanee equipos usando NC

```
luisjordan@kalinetlcj:~$ Archivo Editar Ver Buscar Terminal Ayuda
luisjordan@kalinetlcj:~$ sudo nc 192.168.1.105 135
[sudo] password for luisjordan:
^C
luisjordan@kalinetlcj:~$ sudo nc 192.168.1.105 49154
[  ]
```

The terminal window shows the user running netcat (nc) on port 135 and 49154 of the host 192.168.1.105. The user is prompted for a sudo password.



```

C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\LuCh0>NETSTAT
Conexiones activas

  Proto  Dirección local        Dirección remota      Estado
  TCP    192.168.1.105:2869   192.168.1.103:39310  CLOSE_WAIT
  TCP    192.168.1.105:49154  192.168.1.111:51324  ESTABLISHED
  TCP    192.168.1.105:49212  49.51.229.169:http   ESTABLISHED
  TCP    192.168.1.105:49245  vg-in-f125:5222    ESTABLISHED
  TCP    192.168.1.105:49246  bog02s05-in-f202:https CLOSE_WAIT
  TCP    192.168.1.105:49247  bog02s05-in-f202:https CLOSE_WAIT
  TCP    192.168.1.105:49394  vh-in-f188:5228    ESTABLISHED
  TCP    192.168.1.105:49599  bog02s06-in-f10:https CLOSE_WAIT
  TCP    192.168.1.105:50227  192.168.1.102:8889  ESTABLISHED
  TCP    192.168.1.105:50547  ec2-52-205-213-179:https ESTABLISHED
  TCP    192.168.1.105:50667  gru06s09-in-f101:https ESTABLISHED
  TCP    192.168.1.105:50686  218.93.250.18:http  SYN_SENT
  TCP    192.168.1.105:50688  bog02s07-in-f14:https  ESTABLISHED

C:\Users\LuCh0>_

```

f. Con la herramienta nslookup escanee el dominio cotecnova.edu.co

```

luisjordan@kalinetlcj:~$ nslookup cotecnova.edu.co
Server:      192.168.1.254
Address:      192.168.1.254#53

Non-authoritative answer:
Name:  cotecnova.edu.co
Address: 186.0.53.31

luisjordan@kalinetlcj:~$ 

```

```

luisjordan@kalinetlcj:~$ sudo nslookup -type=any cotecnova.edu.co
Server:      8.8.8.8
Address:      8.8.8.8#53

Non-authoritative answer:
cotecnova.edu.co
origin = ns1.cdmmon.net
mail addr = hostmaster.cotecnova.edu.co
serial = 1372373235
refresh = 10000
retry = 3600
expire = 604800
minimum = 21600
cotecnova.edu.co      nameserver = ns5.cdmndns-01.com.
cotecnova.edu.co      nameserver = ns2.cdmmon.net.
cotecnova.edu.co      nameserver = ns3.cdmmon.net.
cotecnova.edu.co      nameserver = ns4.cdmndns-01.org.
cotecnova.edu.co      nameserver = ns1.cdmmon.net.
cotecnova.edu.co      text = "v=spf1 mx ptr mx:aspmx.l.google.com ip4:74.125.47.27 -all"
cotecnova.edu.co      mail exchanger = 10 ASPMX.L.GOOGLE.com.
Name:  cotecnova.edu.co
Address: 186.0.53.31

Authoritative answers can be found from:

luisjordan@kalinetlcj:~$ sudo nslookup -type=ns cotecnova.edu.co
Server:      8.8.8.8
Address:      8.8.8.8#53

Non-authoritative answer:
cotecnova.edu.co      nameserver = ns2.cdmmon.net.
cotecnova.edu.co      nameserver = ns4.cdmndns-01.org.
cotecnova.edu.co      nameserver = ns5.cdmndns-01.com.
cotecnova.edu.co      nameserver = ns1.cdmmon.net.
cotecnova.edu.co      nameserver = ns3.cdmmon.net.

Authoritative answers can be found from:

```

```

luisjordan@kalinetcj:~ 
Archivo Editar Ver Buscar Terminal Ayuda
cotecnova.edu.co      nameserver = ns1.cdmon.net.
cotecnova.edu.co      nameserver = ns3.cdmon.net.
                                     sistema
Authoritative answers can be found from:
luisjordan@kalinetcj:~$ sudo nslookup -type=mx cotecnova.edu.co
Server:     8.8.8.8
Address:   8.8.8.8#53

Non-authoritative answer:
cotecnova.edu.co      mail exchanger = 10 ASPMX.L.GOOGLE.COM.

Authoritative answers can be found from:
luisjordan@kalinetcj:~$ sudo nslookup -type=soa cotecnova.edu.co
Server:     8.8.8.8
Address:   8.8.8.8#53

Non-authoritative answer:
cotecnova.edu.co
    origin = ns1.cdmon.net
    mail addr = hostmaster.cotecnova.edu.co
    serial = 1372373235
    refresh = 10000
    retry = 3600
    expire = 604800
    minimum = 21600

Authoritative answers can be found from:
luisjordan@kalinetcj:~$ sudo nslookup -debug cotecnova.edu.co
Server:     8.8.8.8
Address:   8.8.8.8#53

Non-authoritative answer:
Name:  cotecnova.edu.co
Address: 186.0.53.31

luisjordan@kalinetcj:~$ 

```

g. Aplicar dig y dnsenum en el dominio cotecnova.edu.co, comparar la información

```

luisjordan@kalinetcj:~ 
Archivo Editar Ver Buscar Terminal Ayuda
luisjordan@kalinetcj:~$ sudo dig cotecnova.edu.co
; <>> DiG 9.11.3-1-Debian <>> cotecnova.edu.co
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19286
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cotecnova.edu.co.           IN      A
;; ANSWER SECTION:
cotecnova.edu.co.     899     IN      A      186.0.53.31

;; Query time: 179 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Apr 29 11:31:51 -05 2018
;; MSG SIZE rcvd: 61

luisjordan@kalinetcj:~$ sudo dnsenum cotecnova.edu.co
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4

----- cotecnova.edu.co -----

Host's addresses:

cotecnova.edu.co.          878     IN      A      186.0.53.31

Wildcard detection using: ooluffxhdpfp
ooluffxhdpfp.cotecnova.edu.co.    899     IN      CNAME   cotecnova.edu.co.


```

```

luisjordan@kalinetcj: ~
Archivo Editar Ver Buscar Terminal Ayuda
luisjordan@kalinetcj:~$ sudo dnsenum cotecnova.edu.co
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4

----- cotecnova.edu.co -----

Host's addresses:

cotecnova.edu.co.          878      IN   A    186.0.53.31

Wildcard detection using: ooluffxhdpgp

ooluffxhdpgp.cotecnova.edu.co. 899      IN   CNAME  cotecnova.edu.co.
cotecnova.edu.co.           878      IN   A    186.0.53.31

!!!!!!!!

Wildcards detected, all subdomains will point to the same IP address
Omitting results containing 186.0.53.31.
Maybe you are using OpenDNS servers.
!!!!!!!!

Name Servers:

ns2.cdmون.net.          6325     IN   A    35.195.57.29
ns5.cdmونdns-01.com.    899      IN   A    52.59.146.62
ns1.cdmون.net.          3066     IN   A    35.189.106.232
ns4.cdmونdns-01.org.    899      IN   A    52.58.66.183
ns3.cdmون.net.          19209    IN   A    35.157.47.125

```

```

luisjordan@kalinetcj: ~
Archivo Editar Ver Buscar Terminal Ayuda
Documentos   Monitor del sistema
Name Servers:

ns2.cdmون.net.          6325     IN   A    35.195.57.29
ns5.cdmونdns-01.com.    899      IN   A    52.59.146.62
ns1.cdmون.net.          3066     IN   A    35.189.106.232
ns4.cdmونdns-01.org.    899      IN   A    52.58.66.183
ns3.cdmون.net.          19209    IN   A    35.157.47.125

Mail (MX) Servers:

ASPMX.L.GOOGLE.COM.     292      IN   A    74.125.141.27

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for cotecnova.edu.co on ns2.cdmون.net ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for cotecnova.edu.co on ns5.cdmونdns-01.com ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for cotecnova.edu.co on ns1.cdmون.net ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for cotecnova.edu.co on ns4.cdmونdns-01.org ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for cotecnova.edu.co on ns3.cdmون.net ...
AXFR record query failed: NOTAUTH

brute force file not specified, bay.
luisjordan@kalinetcj:~$ 

```

- h. Resuma en un cuadro comparativo la información más importante que considere obtuvo de este proceso que le servirá para una auditoría y con qué herramientas la obtuvo.

Es importante obtener una previa información del host destino al que se pretende realizar una auditoría de seguridad. Dentro de esta información se encuentran las piezas claves por donde se pueden realizar las penetraciones al sistema. Cabe aclarar que estos procedimientos deben únicamente con el propósito de auditar la seguridad de la información de la red.

INFORMACIÓN A RECOLECTAR	OBSERVACIÓN
Ingeniería Social	Método para obtener información del host de destino haciendo uso de las redes sociales o simplemente conociendo las personas que administran la red con el fin de encontrar indicios de brechas de seguridad.
Conocer a qué se dedican	Conocer con qué fin se usa el servidor, y que muchas veces, las empresas usan 1 solo servidor para múltiples servicios y también las hay que tienen un servidor específico para cada labor en la compañía.

Recolestad la información anterior, es necesario elegir las herramientas de software con las que se pretende recolectar la información lógica de los equipos o equipo a auditar.

HERRAMIENTA	DESCRIPCIÓN

DIG y DNSENUM	Con estas utilidades, podremos analizar la información pública de la red, tal como lo es el dominio y los registros de este en otros servidores DNS al igual que entradas de correo y saltos de la red.
NMAP	Herramienta utilizada para escanear las propiedades de la red y de los equipos que en ella se encuentran, con el fin de obtener en una consola la mayor información de puertos disponibles en la red, cantidad de equipos y si cuentan con seguridad perimetral o algún tipo de filtrado de paquetes.
ZENMAP	Esta herramienta, se complementa con NMAP ya que de una manera gráfica, nos va a mostrar mayor información al respecto del estado de la red.
ARP	Una vez dentro de la red, con esta herramienta, nos va a permitir obtener las direcciones MAC de los equipos que se encuentran disponibles en la red con el propósito inicial de que en caso de haber filtrado MAC, haciendo el clonado de una de estas nos pueda permitir el acceso normal a la red.

WIRESHARK	Haciendo uso de esta utilidad, nos permitirá ver en tiempo real los paquetes que circulan por la red, en búsqueda de una vulnerabilidad de seguridad y encontrar alguna clave enviada sin cifrado o datos importantes.
-----------	--

3. Análisis de Vulnerabilidades:

- a. Aplicando una herramienta como nessus realice un escaneo de red y completo, que me permita obtener información de vulnerabilidades de un equipo.

R//En este punto se anexa documento PDF, en el cual muestra un análisis completo al dominio.