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

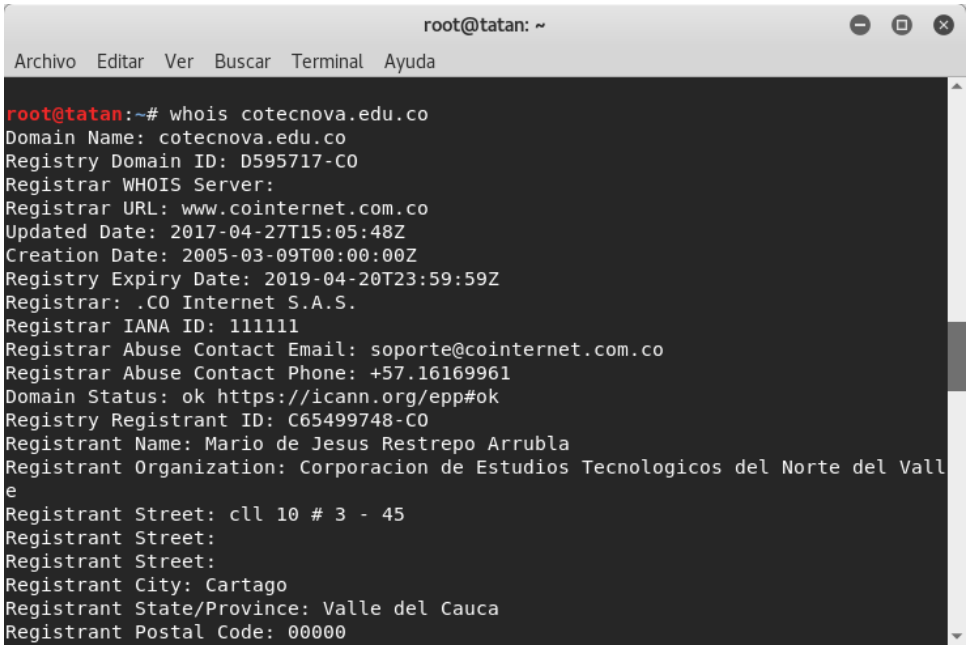
SEMESTRE V

2018

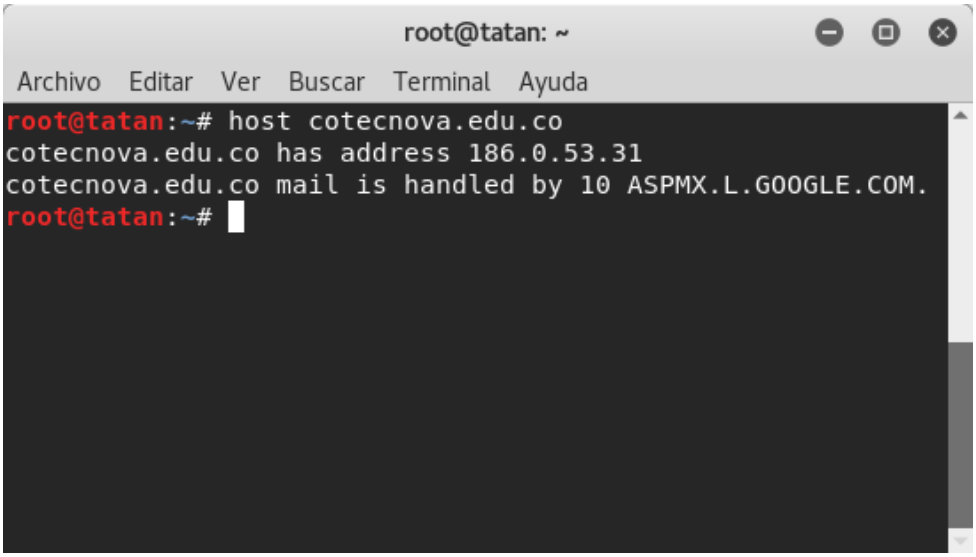
TALLER

1. Obtención de información:

a. Usando el protocolo whois, realizar el analisis del dominio cotecnova.edu.co

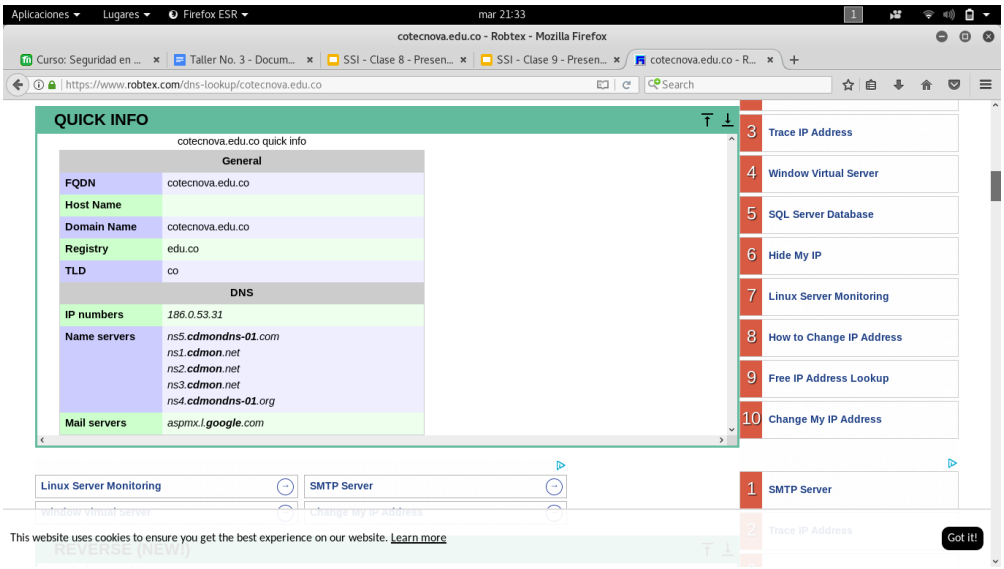


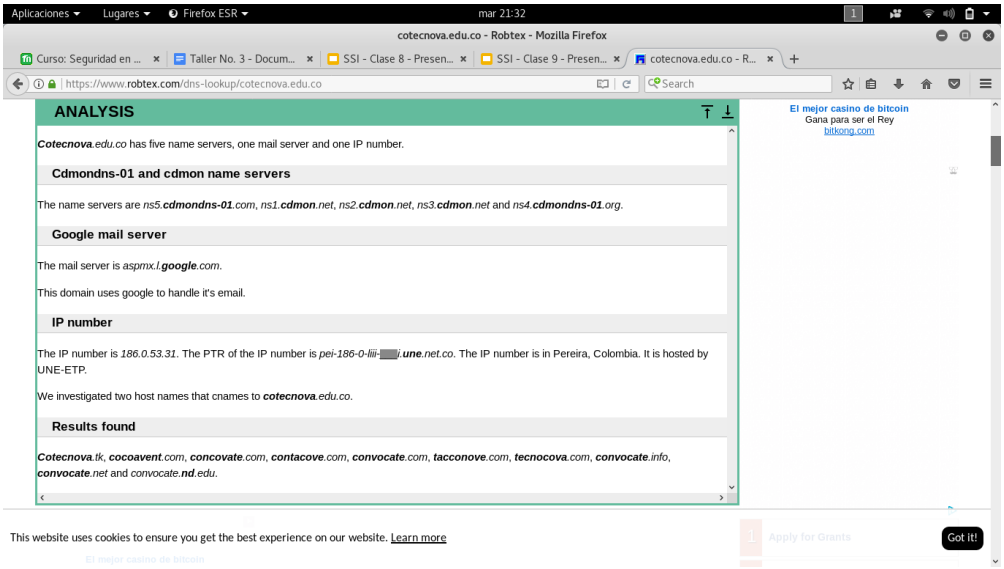
b. Usando el protocolo host, realizar el analisis del dominio cotecnova.edu.co



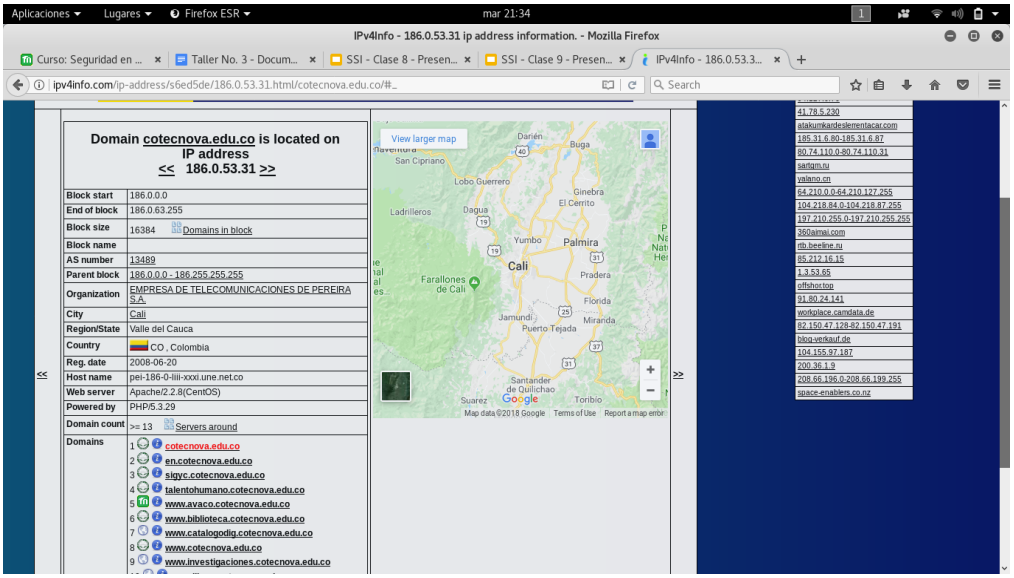
c. Usando el dominio cotecnova.edu.co usar los siguientes sitios indicando cual es la diferencia de la información que entrega cada una de ellos:

Robtex:

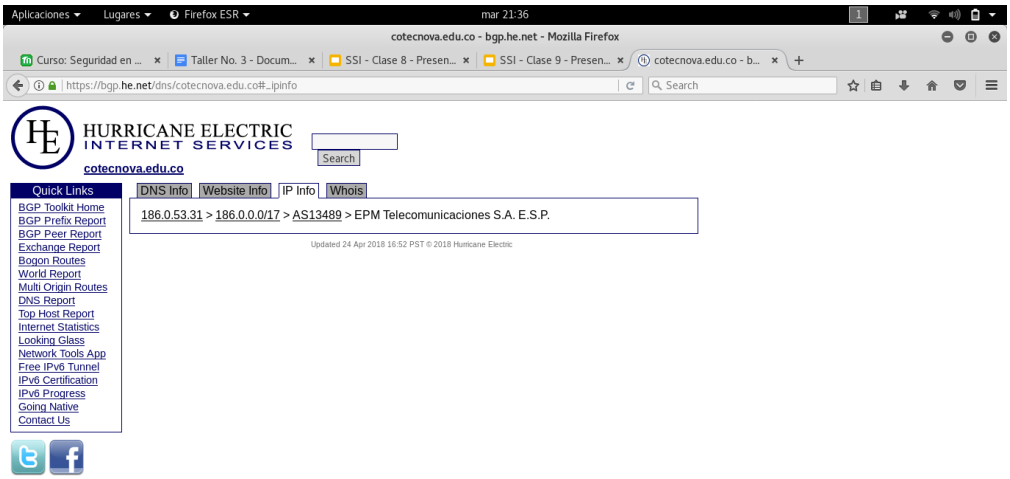




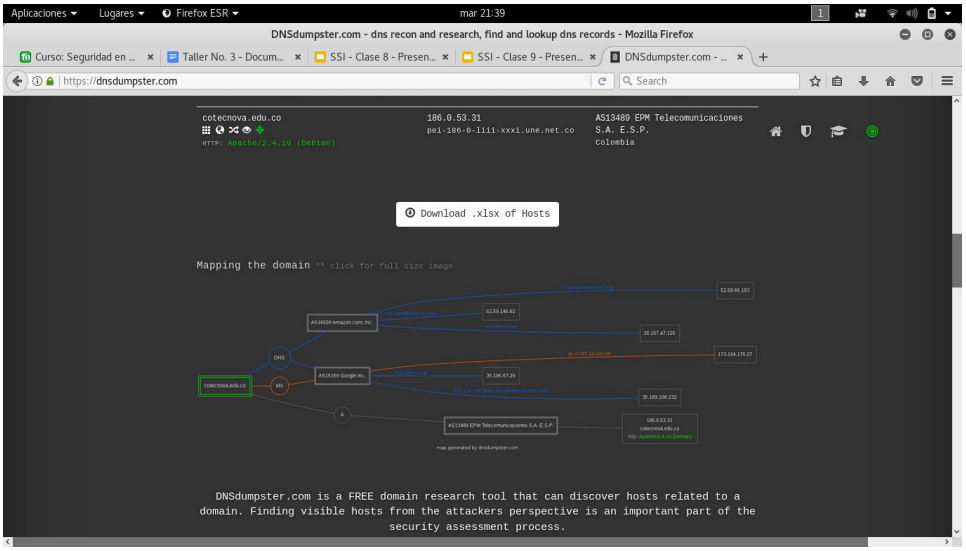
Ipv4info:



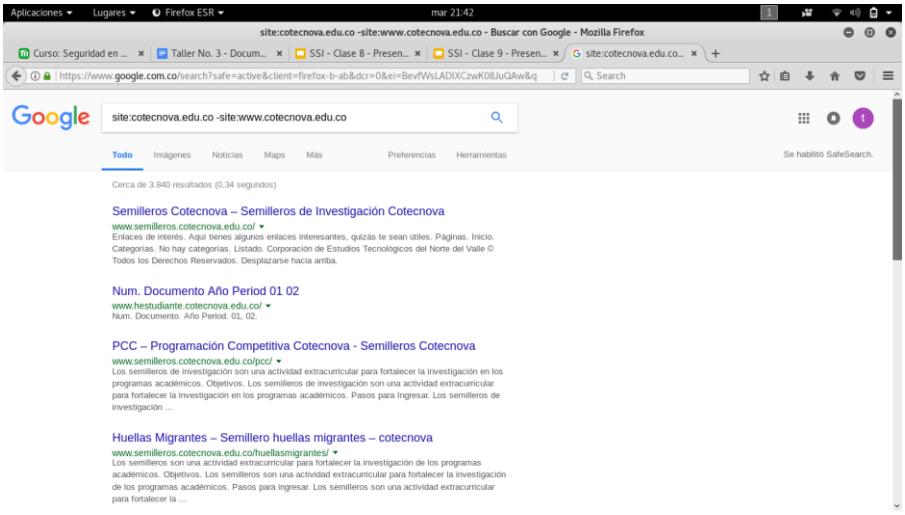
Bgp hurricane:

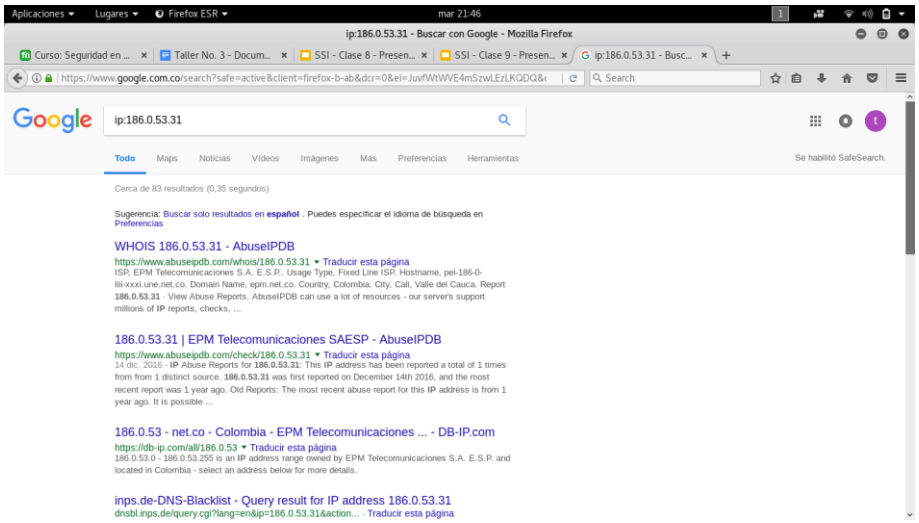


Dnsdumpster:

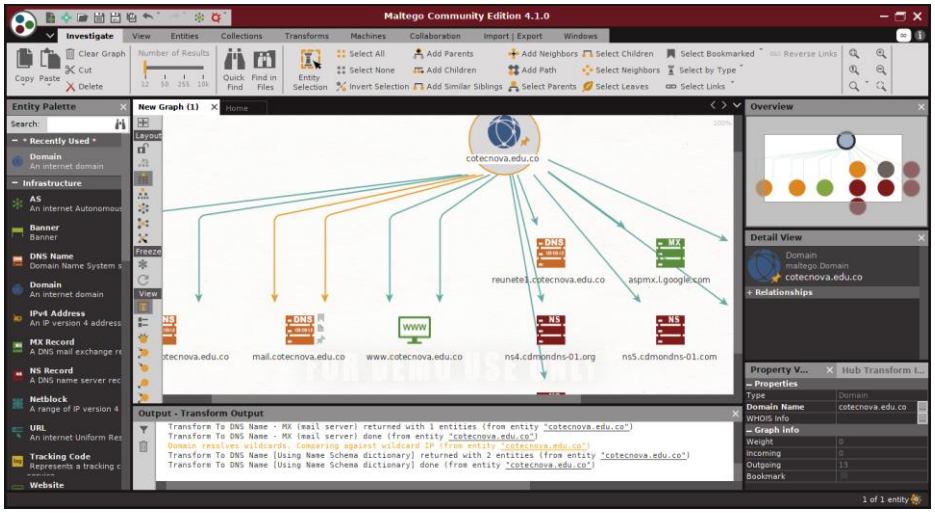


d. Aplicar las técnicas de browser hacking con google y buscar la información disponible de la cotecnova.edu.co

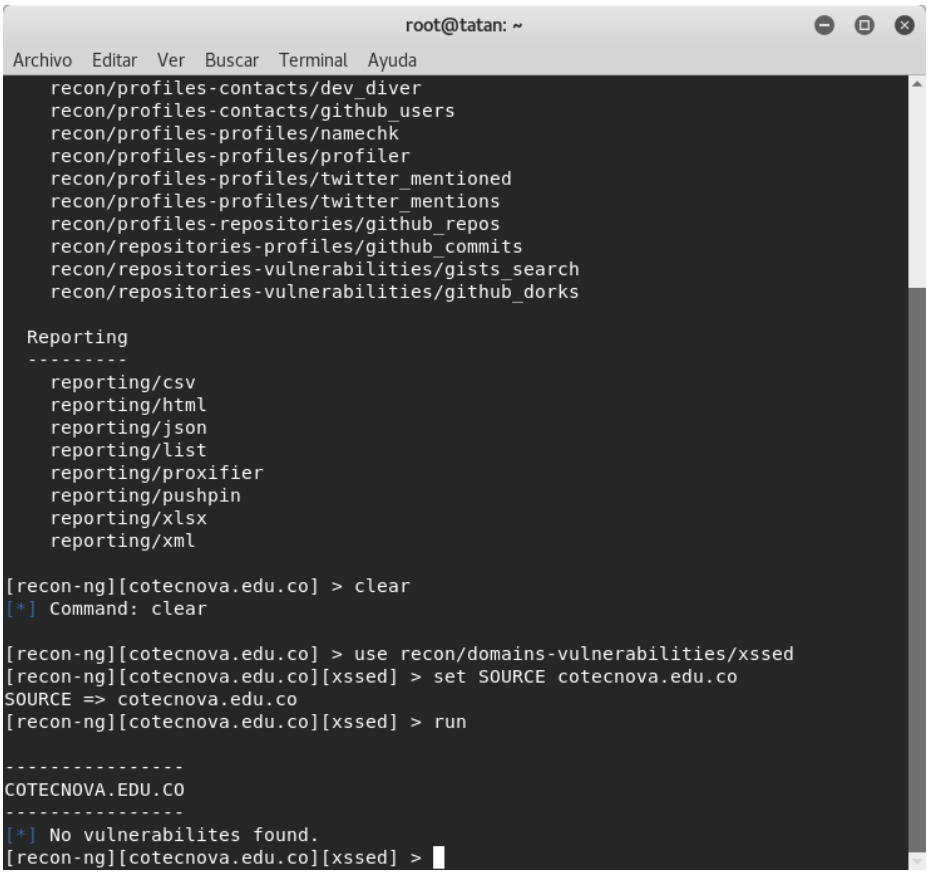




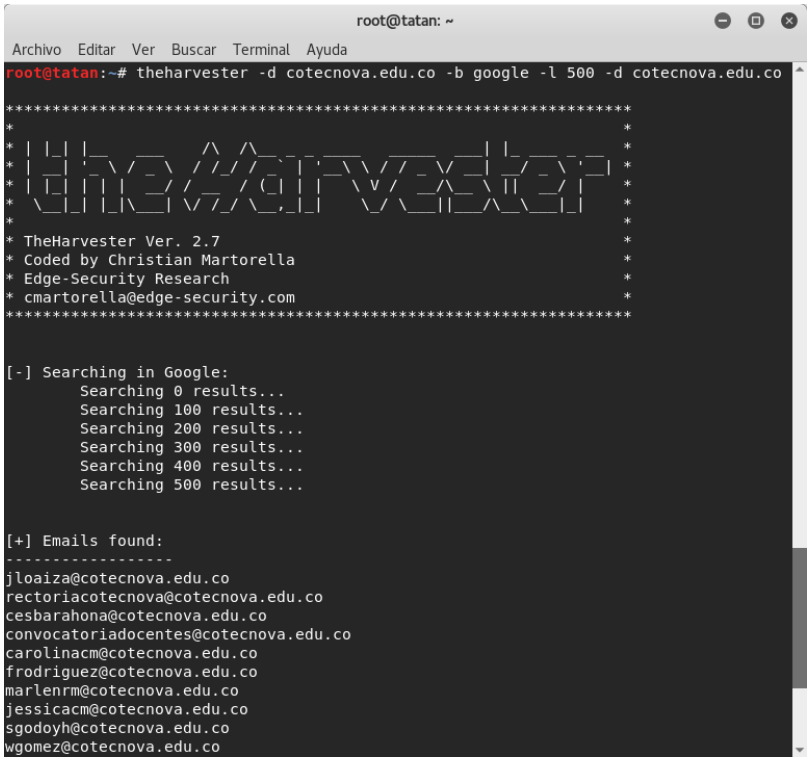
e. Aplicando maltego obtener la información del dominio cotecnova.edu.co

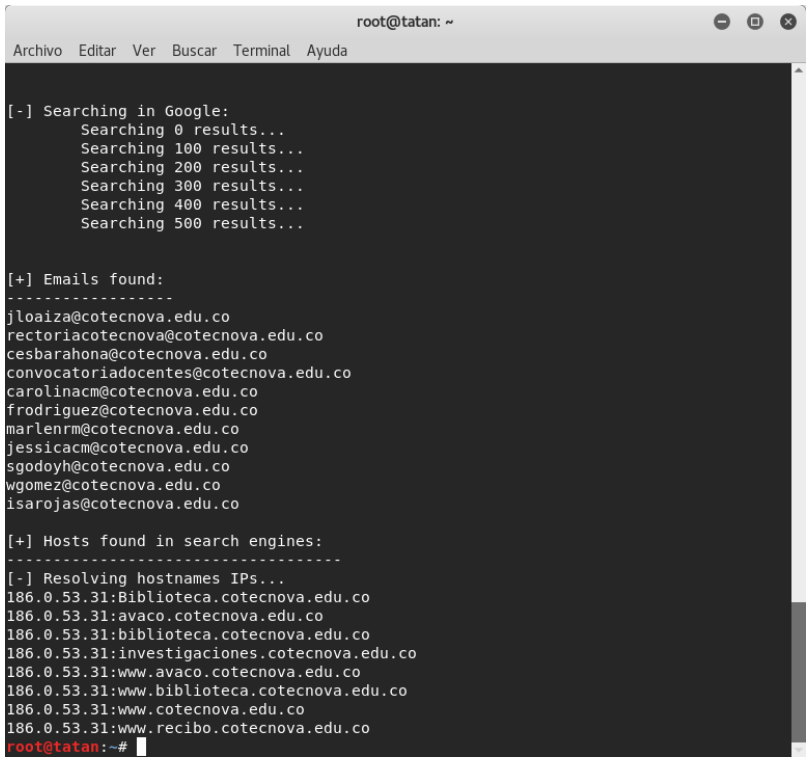


f. Usando recon-ng aplicar un módulo que permita obtener información importante del dominio cotecnova.edu.co

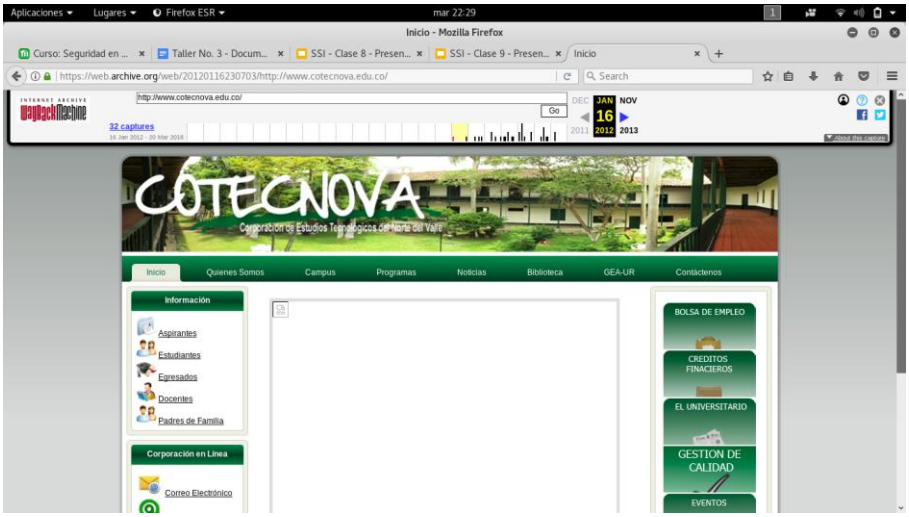


g. Use theharvester para obtener información adicional a su proceso de investigación del dominio cotecnova.edu.co

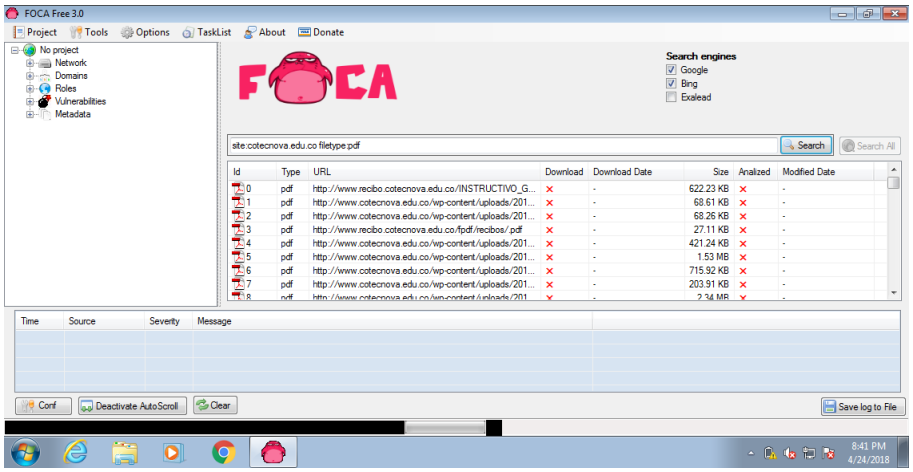




h. Consulte archive.org y obtenga información importante sobres las diferentes versiones que ha tenido el dominio cotecnova.edu.co



i. Usando foca analice por lo menos archivos del dominio cotecnova.edu.co



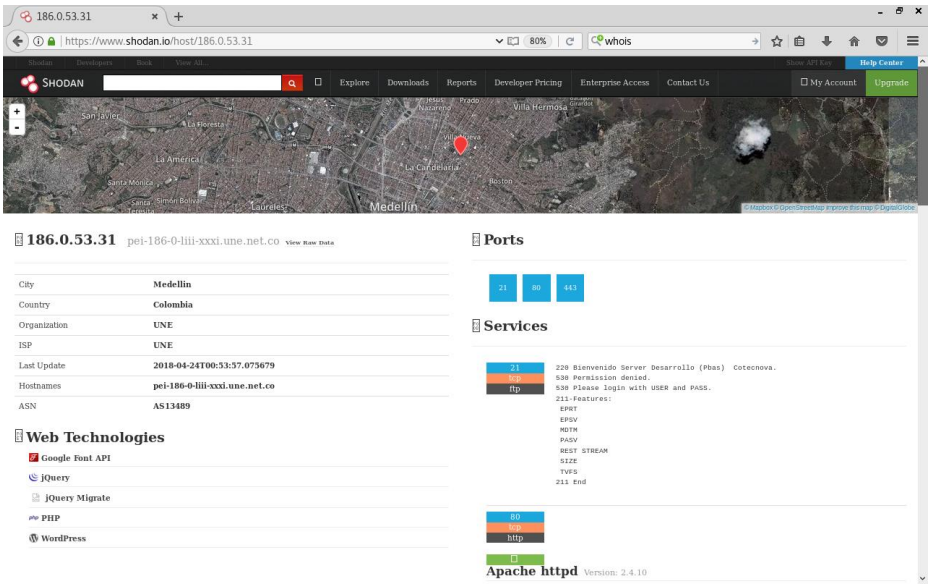
j. Resuma en un cuadro comparativo la información más importante que considere obtuvo de este proceso que le servirá para una auditoría y con qué herramienta la obtuvo.

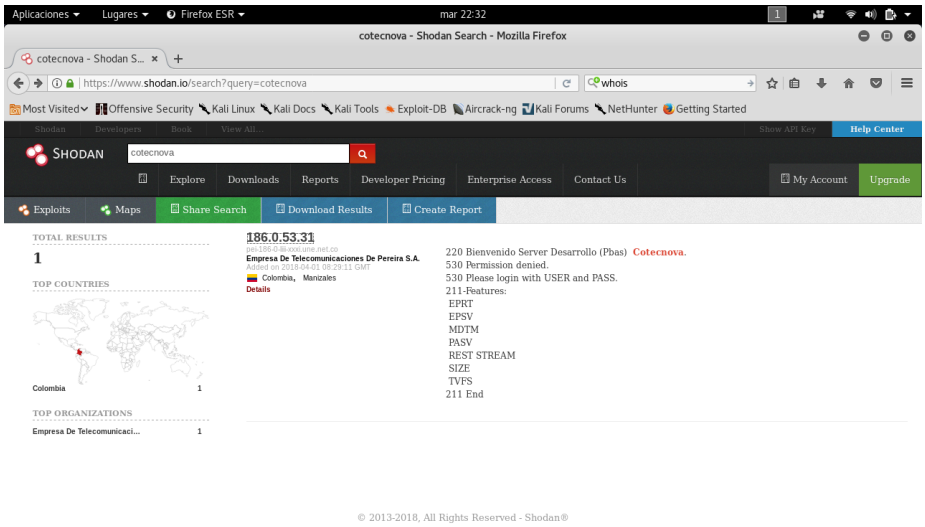
k.

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.

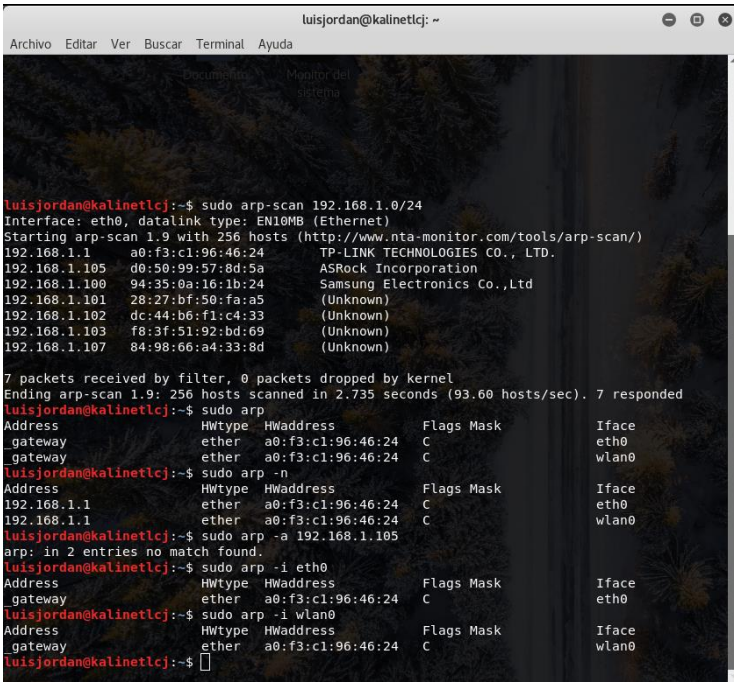
2. Enumeración de Sistemas:

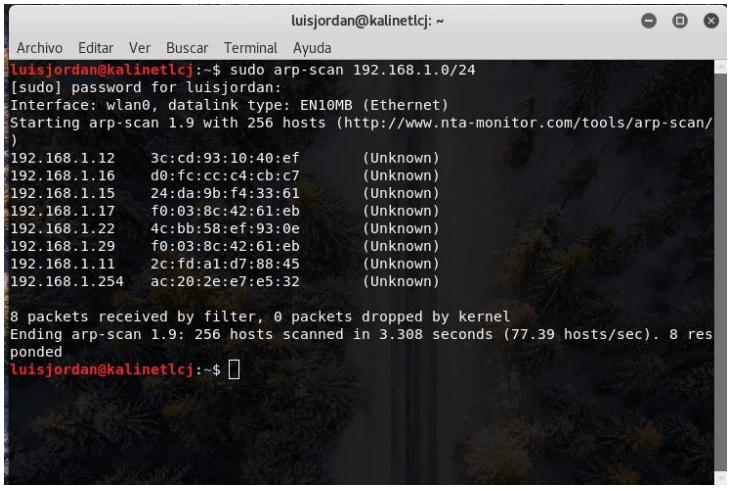
a. Consultar en shodan la información que pueda obtener del dominio cotecnova.edu.co

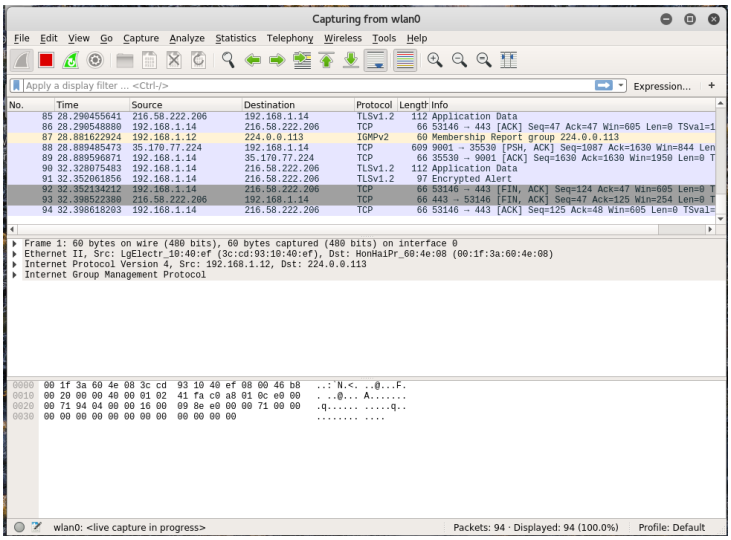




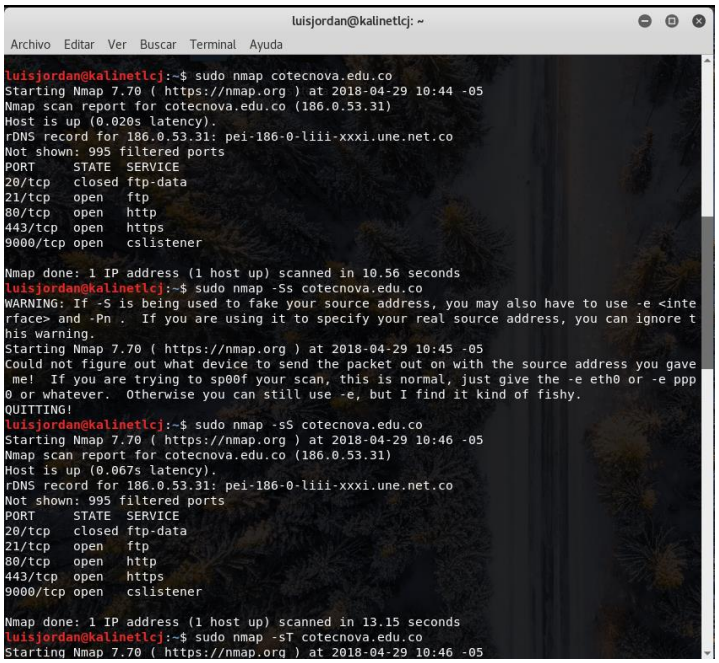
b. Realice un escaneo usando arp, arp-scan, wireshark

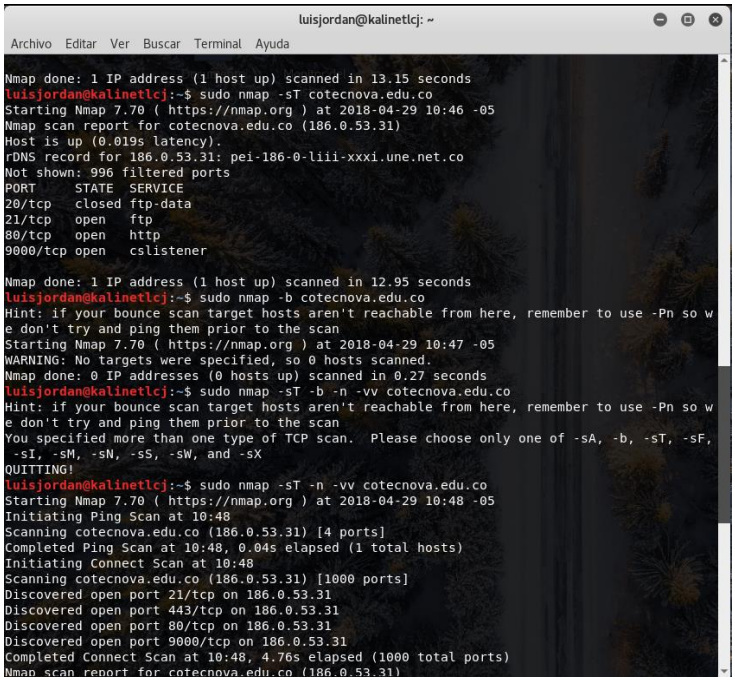

luisjordan@kalinetlcj: ~
Archivo Editar Ver Buscar Terminal Ayuda
luisjordan@kalinetlcj:~$ sudo arp-scan 192.168.1.0/24
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.1.1 a0:f3:c1:96:46:24 TP-LINK TECHNOLOGIES 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@kalinetlcj:~$ 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@kalinetlcj:~$ 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@kalinetlcj:~$ sudo arp -a 192.168.1.105
arp: in 2 entries no match found.
luisjordan@kalinetlcj:~$ sudo arp -i eth0
Address HWtype HWaddress Flags Mask Iface
_gateway ether a0:f3:c1:96:46:24 C eth0
luisjordan@kalinetlcj:~$ sudo arp -i wlan0
Address HWtype HWaddress Flags Mask Iface
_gateway ether a0:f3:c1:96:46:24 C wlan0
luisjordan@kalinetlcj:~$

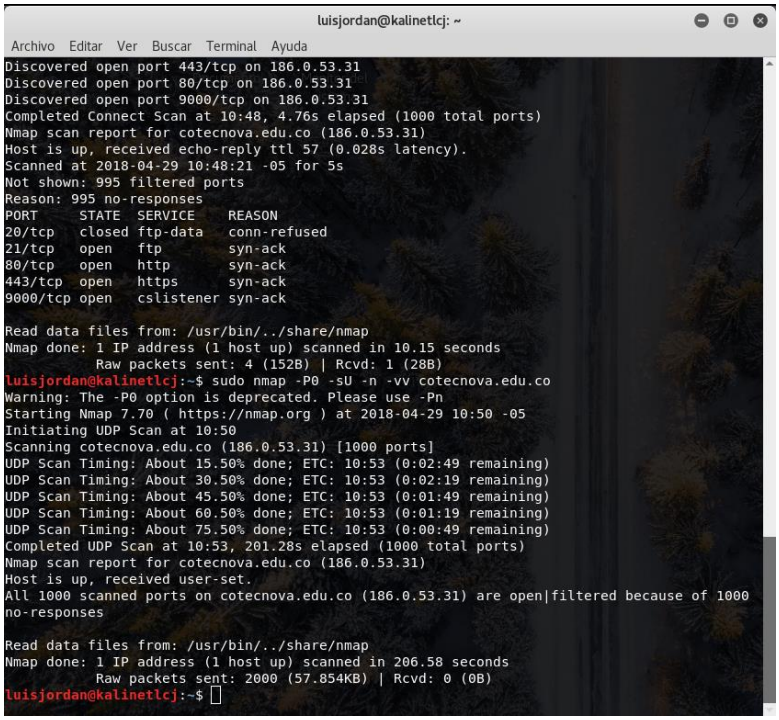

luisjordan@kalinetlcj: ~
Archivo Editar Ver Buscar Terminal Ayuda
luisjordan@kalinetlcj:~$ sudo arp-scan 192.168.1.0/24
[sudo] password for luisjordan:
Interface: wlan0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.1.12 3c:cd:93:10:40:ef (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 responded
luisjordan@kalinetlcj:~$

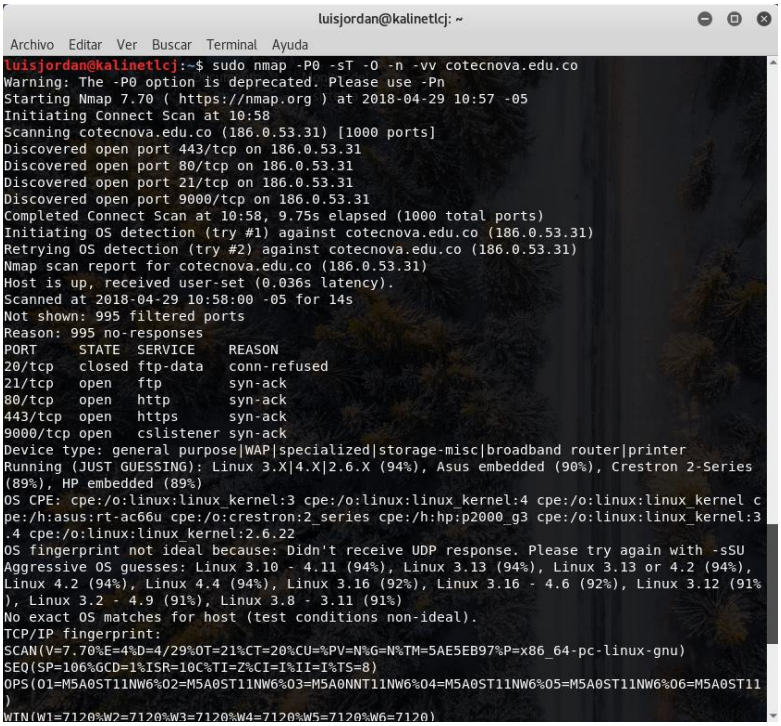

Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
85 28.290455641 216.58.222.206 192.168.1.14 TLSv1.2 112 Application Data
86 28.290548880 192.168.1.14 216.58.222.206 TCP 66 53146 → 443 [ACK] Seq=47 Ack=47 Win=605 Len=0 TSval=1
87 28.881622924 192.168.1.12 224.0.0.113 IGMPv2 60 Membership Report group 224.0.0.113
88 28.889485473 35.170.77.224 192.168.1.14 TCP 609 9001 → 35530 [PSH, ACK] Seq=1087 Ack=1630 Win=844 Len
89 28.889596871 192.168.1.14 35.170.77.224 TCP 66 35530 → 9001 [ACK] Seq=1630 Ack=1630 Win=1950 Len=0 T
90 32.328075483 192.168.1.14 216.58.222.206 TLSv1.2 112 Application Data
91 32.352061856 192.168.1.14 216.58.222.206 TLSv1.2 97 Encrypted Alert
92 32.352134212 192.168.1.14 216.58.222.206 TCP 66 53146 → 443 [FIN, ACK] Seq=124 Ack=47 Win=605 Len=0 T
93 32.398522380 216.58.222.206 192.168.1.14 TCP 66 443 → 53146 [FIN, ACK] Seq=47 Ack=125 Win=254 Len=0 T
94 32.398618203 192.168.1.14 216.58.222.206 TCP 66 53146 → 443 [ACK] Seq=125 Ack=48 Win=605 Len=0 TSval=
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: LgElectr_10:40:ef (3c:cd:93:10:40:ef), Dst: HonHaiPr_60:4e:08 (00:1f:3a:60:4e:08)
Internet Protocol Version 4, Src: 192.168.1.12, Dst: 224.0.0.113
Internet Group Management Protocol
0000 00 1f 3a 60 4e 08 3c cd 93 10 40 ef 08 00 46 b8 ..:`N.<. ..@...F.
0010 00 20 00 00 40 00 01 02 41 fa c0 a8 01 0c e0 00 . ..@... A.......
0020 00 71 94 04 00 00 16 00 09 8e e0 00 00 71 00 00 .q..... .....q..
0030 00 00 00 00 00 00 00 00 00 00 00 00 ....
wlan0: <live capture in progress>
Packets: 94 · Displayed: 94 (100.0%)
Profile: Default

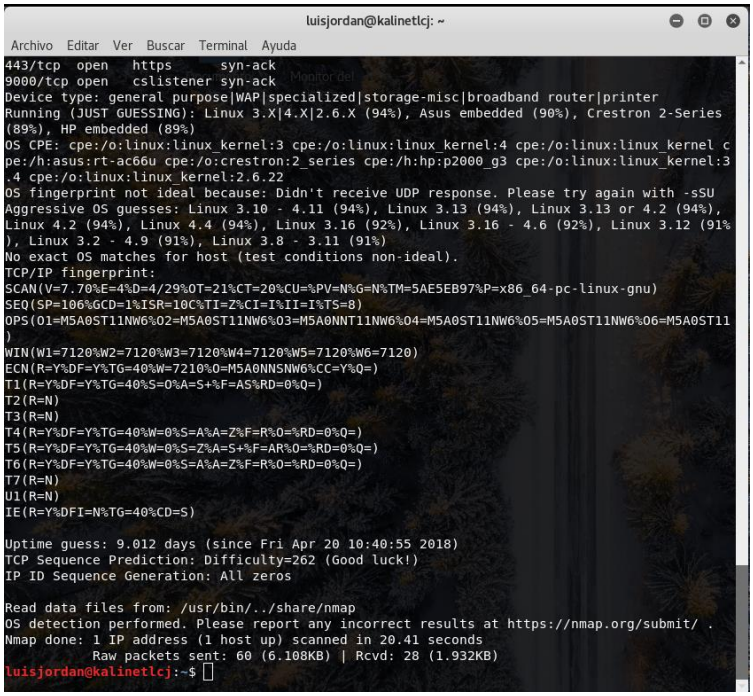
c. Realizar un escaneo profundo de la red usando la herramienta nmap que permita obtener información importante



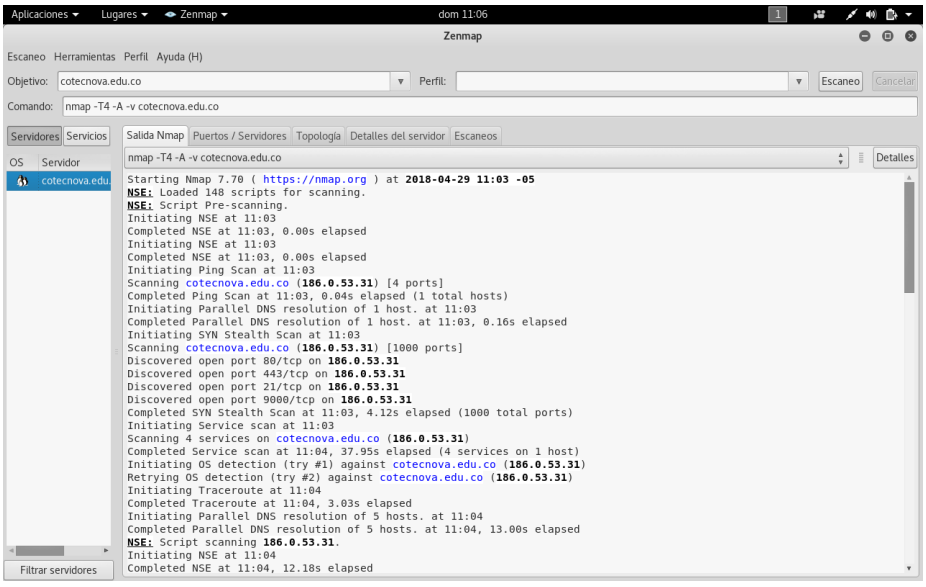


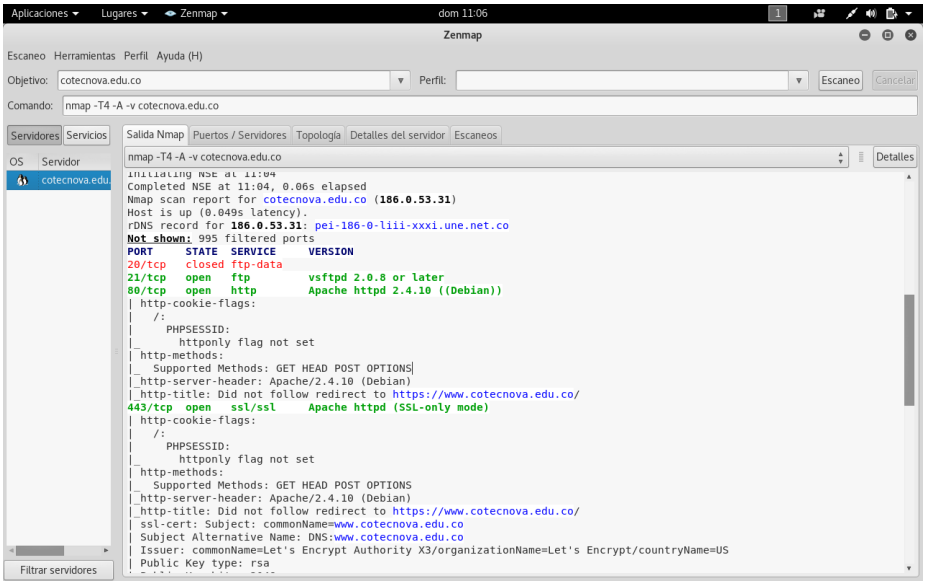

luisjordan@kalinetlcj: ~
Archivo Editar Ver Buscar Terminal Ayuda
Discovered open port 443/tcp on 186.0.53.31
Discovered open port 80/tcp on 186.0.53.31
Discovered open port 9000/tcp on 186.0.53.31
Completed Connect Scan at 10:48, 4.76s elapsed (1000 total ports)
Nmap scan report for cotecnova.edu.co (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 7.70 (https://nmap.org) at 2018-04-29 10:50 -05
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:~$

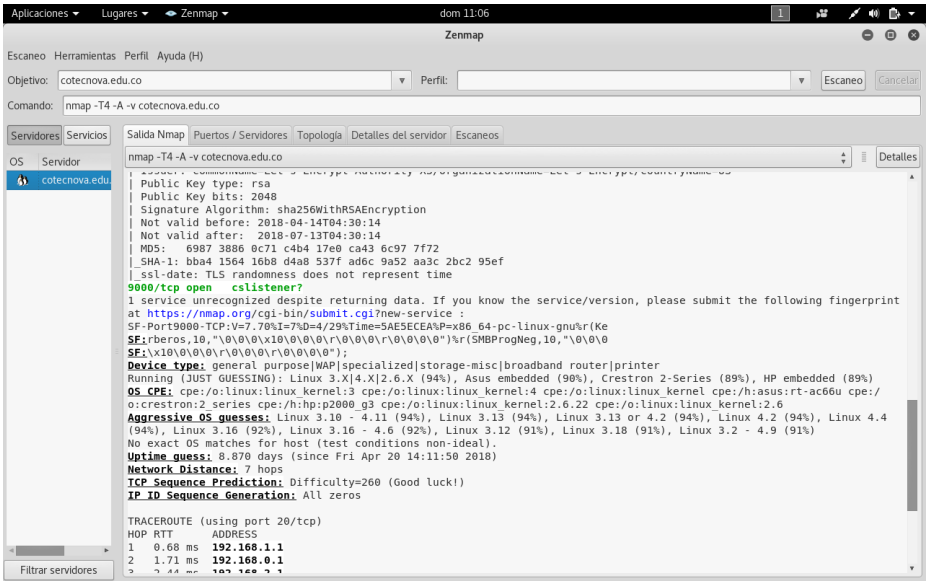

luisjordan@kalinetlcj: ~
Archivo Editar Ver Buscar Terminal Ayuda
luisjordan@kalinetlcj:~$ sudo nmap -P0 -sT -O -n -vv cotecnova.edu.co
Warning: The -P0 option is deprecated. Please use -Pn
Starting Nmap 7.70 (https://nmap.org) at 2018-04-29 10:57 -05
Initiating Connect Scan at 10:58
Scanning cotecnova.edu.co (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=%PV=N%G=N%TM=5AE5EB97%P=x86_64-pc-linux-gnu)
SEQ(SP=106%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=8)
OPS(O1=M5A0ST11NW6%O2=M5A0ST11NW6%O3=M5A0NNT11NW6%O4=M5A0ST11NW6%O5=M5A0ST11NW6%O6=M5A0ST11)
WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)

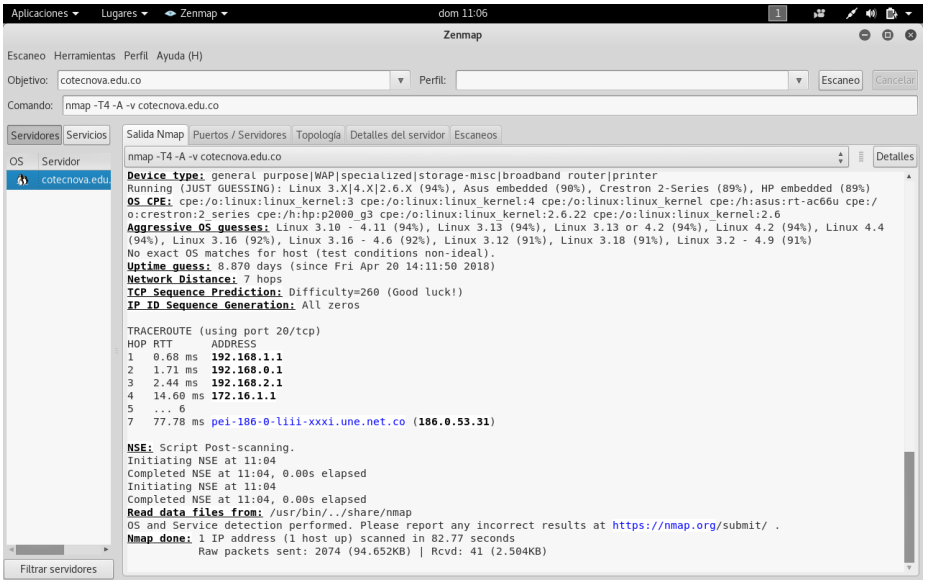


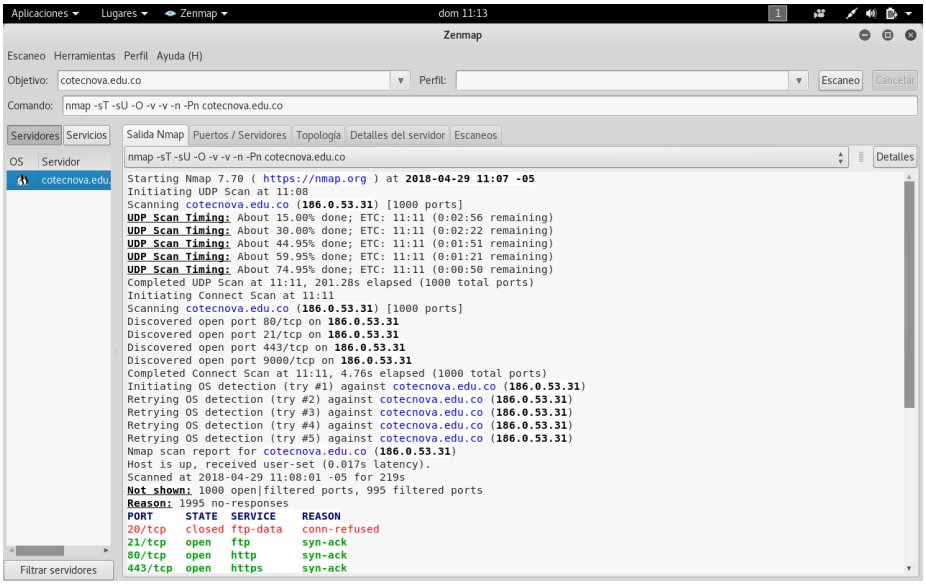
d. Realizar un escaneo profundo de la red usando la herramienta zenmap que permita obtener información importante

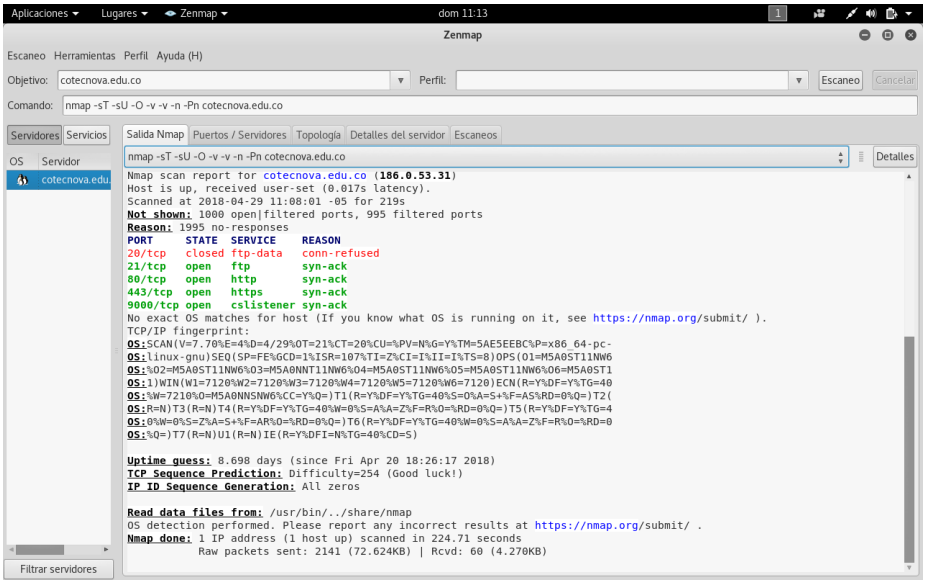


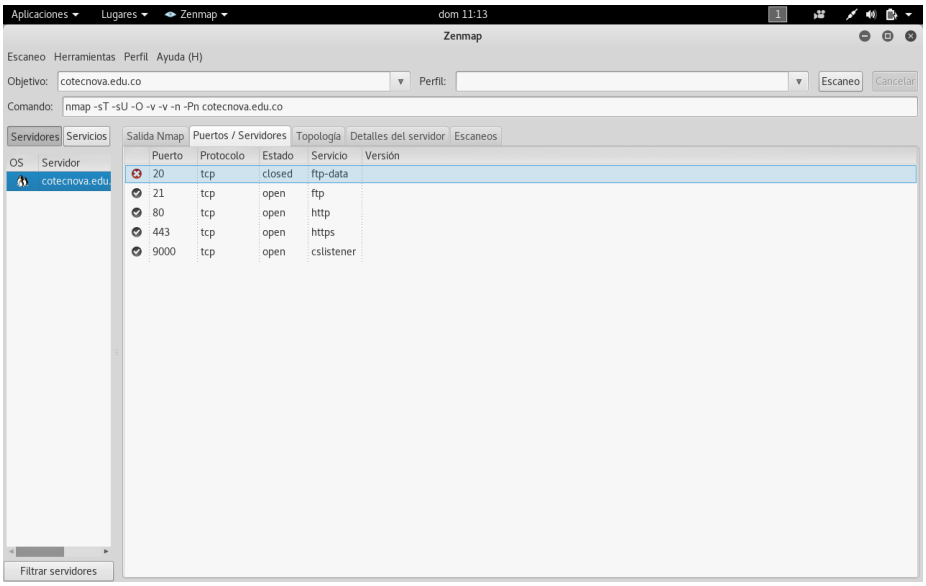

Aplicaciones
Lugares
Zenmap
dom 11:06
Zenmap
Escaneo Herramientas Perfil Ayuda (H)
Objetivo: cotecnova.edu.co
Perfil:
Escaneo
Cancelar
Comando: nmap -T4 -A -v cotecnova.edu.co
Servidores
Servicios
Salida Nmap
Puertos / Servidores
Topología
Detalles del servidor
Escaneos
OS
Servidor
cotecnova.edu
nmap -T4 -A -v cotecnova.edu.co
Detalles
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: pei-186-0-liii-xxxi.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
Filtrar servidores

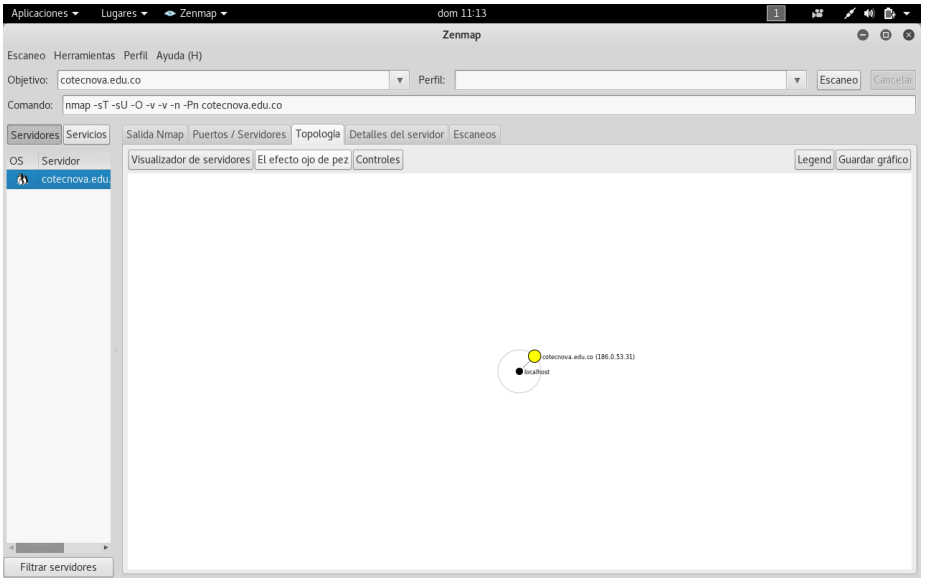

Aplicaciones
Lugares
Zenmap
dom 11:06
Zenmap
Escaneo Herramientas Perfil Ayuda (H)
Objetivo: cotecnova.edu.co
Perfil:
Escaneo
Cancelar
Comando: nmap -T4 -A -v cotecnova.edu.co
Servidores
Servicios
Salida Nmap
Puertos / Servidores
Topología
Detalles del servidor
Escaneos
OS
Servidor
cotecnova.edu
nmap -T4 -A -v cotecnova.edu.co
Detalles
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-04-14T04:30:14
| Not valid after: 2018-07-13T04:30:14
| MD5: 6987 3886 0c71 c4b4 17e0 ca43 6c97 7f72
|_SHA-1: bba4 1564 16b8 d4a8 537f ad6c 9a52 aa3c 2bc2 95ef
|_ssl-date: TLS randomness does not represent time
9000/tcp open cslistener?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9000-TCP:V=7.70%I=7%D=4/29%Time=5AE5ECEA%P=x86_64-pc-linux-gnu%r(Ke
SF:rberos,10,"\0\0\0\x10\0\0\0\r\0\0\0\r\0\0\0\0")%r(SMBProgNeg,10,"\0\0\0
SF:\x10\0\0\0\r\0\0\0\r\0\0\0\0");
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:2.6.22 cpe:/o:linux:linux_kernel:2.6
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 3.18 (91%), Linux 3.2 - 4.9 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 8.870 days (since Fri Apr 20 14:11:50 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
Filtrar servidores

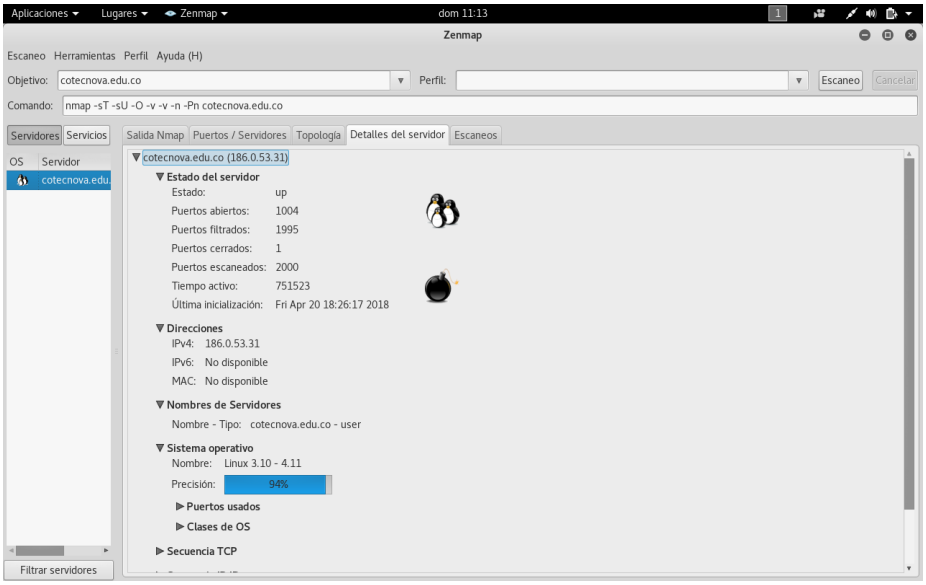

Aplicaciones
Lugares
Zenmap
dom 11:06
Zenmap
Escaneo Herramientas Perfil Ayuda (H)
Objetivo: cotecnova.edu.co
Perfil:
Escaneo
Cancelar
Comando: nmap -T4 -A -v cotecnova.edu.co
Servidores
Servicios
Salida Nmap
Puertos / Servidores
Topología
Detalles del servidor
Escaneos
OS
Servidor
cotecnova.edu
nmap -T4 -A -v cotecnova.edu.co
Detalles
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:2.6.22 cpe:/o:linux:linux_kernel:2.6
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 3.18 (91%), Linux 3.2 - 4.9 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 8.870 days (since Fri Apr 20 14:11:50 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 14.60 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 (1 host up) scanned in 82.77 seconds
Raw packets sent: 2074 (94.652KB) | Rcvd: 41 (2.504KB)
Filtrar servidores

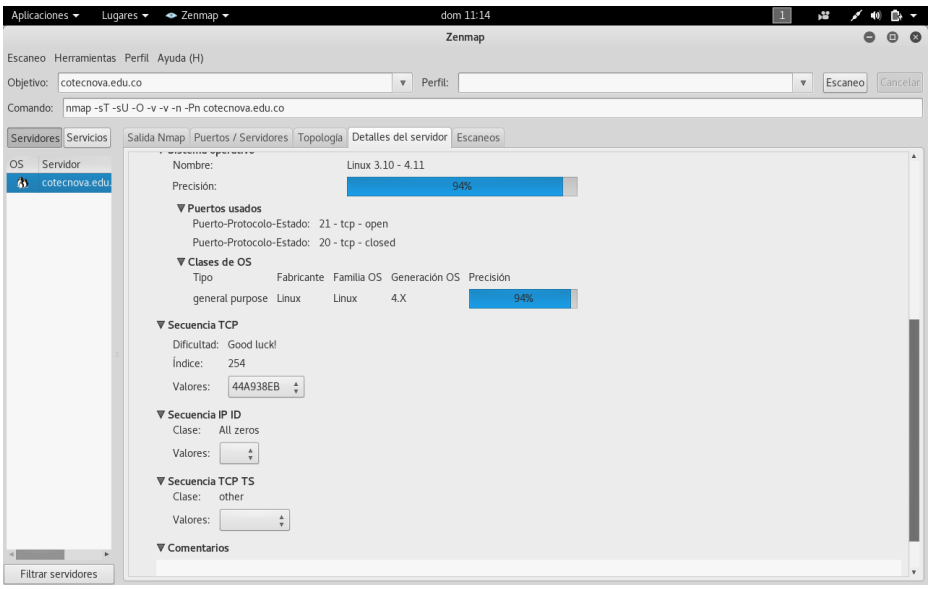

Aplicaciones Lugares Zenmap dom 11:13
Zenmap
Escaneo Herramientas Perfil Ayuda (H)
Objetivo: cotecnova.edu.co
Perfil:
Escaneo
Cancelar
Comando: nmap -sT -sU -O -v -v -n -Pn cotecnova.edu.co
Servidores Servicios
OS Servidor
cotecnova.edu
Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos
nmap -sT -sU -O -v -v -n -Pn cotecnova.edu.co
Detalles
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
Scanning cotecnova.edu.co (186.0.53.31) [1000 ports]
Discovered open port 80/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 report for cotecnova.edu.co (186.0.53.31)
Host is up, received user-set (0.017s latency).
Scanned at 2018-04-29 11:08:01 -05 for 219s
Not shown: 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
Filtrar servidores

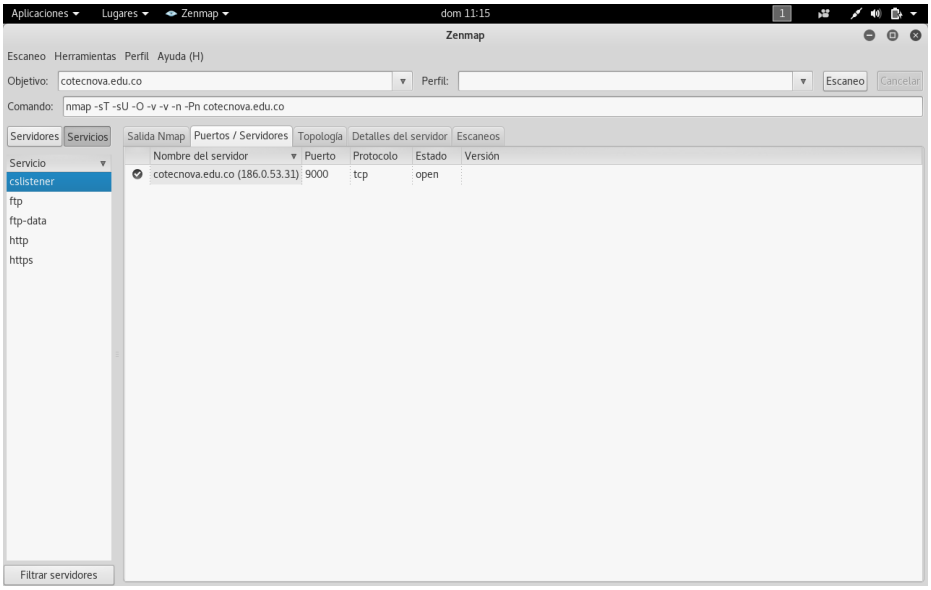

Aplicaciones Lugares Zenmap dom 11:13
Zenmap
Escaneo Herramientas Perfil Ayuda (H)
Objetivo: cotecnova.edu.co
Perfil:
Escaneo
Cancelar
Comando: nmap -sT -sU -O -v -v -n -Pn cotecnova.edu.co
Servidores Servicios
OS Servidor
cotecnova.edu
Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos
nmap -sT -sU -O -v -v -n -Pn cotecnova.edu.co
Detalles
Nmap scan report for cotecnova.edu.co (186.0.53.31)
Host is up, received user-set (0.017s latency).
Scanned at 2018-04-29 11:08:01 -05 for 219s
Not shown: 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%E=4%D=4/29%OT=21%CT=20%CU=%PV=N%G=Y%TM=5AE5EEBC%P=x86_64-pc-
OS:linux-gnu)SEQ(SP=FE%GCD=1%ISR=107%TI=Z%CI=I%II=I%TS=8)OPS(O1=M5A0ST11NW6
OS:%O2=M5A0ST11NW6%O3=M5A0NNT11NW6%O4=M5A0ST11NW6%O5=M5A0ST11NW6%O6=M5A0ST1
OS:1)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%TG=40
OS:%W=7210%O=M5A0NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)T2(
OS:R=N)T3(R=N)T4(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%TG=4
OS:0%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0
OS:%Q=)T7(R=N)U1(R=N)IE(R=Y%DFI=N%TG=40%CD=S)
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 -v -n -Pn cotecnova.edu.co
Servidores Servicios
OS Servidor
cotecnova.edu
Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos
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

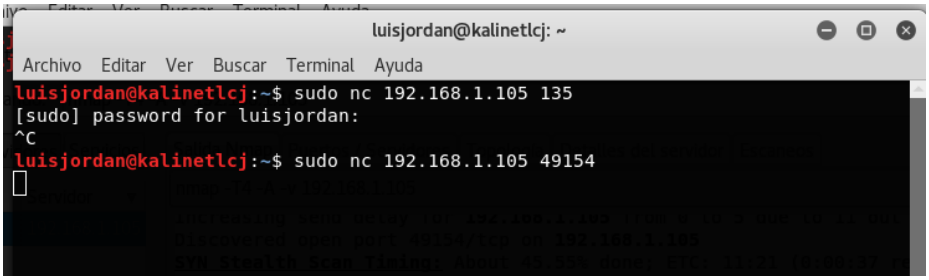

Aplicaciones
Lugares
Zenmap
dom 11:13
Zenmap
Escaneo Herramientas Perfil Ayuda (H)
Objetivo: cotecnova.edu.co
Perfil:
Escaneo
Cancelar
Comando: nmap -sT -sU -O -v -v -n -Pn cotecnova.edu.co
Servidores
Servicios
Salida Nmap
Puertos / Servidores
Topología
Detalles del servidor
Escaneos
OS
Servidor
cotecnova.edu
Visualizador de servidores
El efecto ojo de pez
Controles
Legend
Guardar gráfico
cotecnova.edu.co (186.0.53.31)
localhost
Filtrar servidores

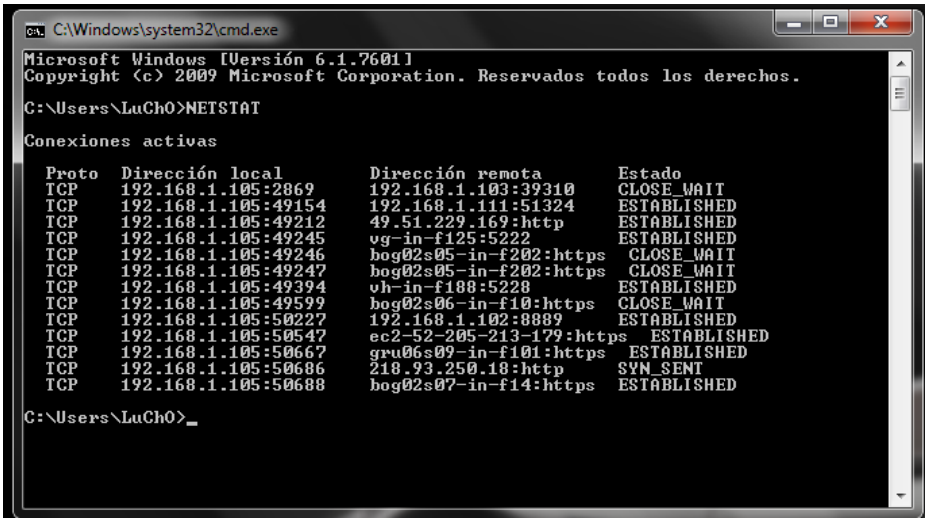

Aplicaciones
Lugares
Zenmap
dom 11:13
Zenmap
Escaneo Herramientas Perfil Ayuda (H)
Objetivo: cotecnova.edu.co
Perfil:
Escaneo
Cancelar
Comando: nmap -sT -sU -O -v -v -n -Pn cotecnova.edu.co
Servidores
Servicios
Salida Nmap
Puertos / Servidores
Topología
Detalles del servidor
Escaneos
OS
Servidor
cotecnova.edu
cotecnova.edu.co (186.0.53.31)
Estado del servidor
Estado: up
Puertos abiertos: 1004
Puertos filtrados: 1995
Puertos cerrados: 1
Puertos escaneados: 2000
Tiempo activo: 751523
Última inicialización: Fri Apr 20 18:26:17 2018
Direcciones
IPv4: 186.0.53.31
IPv6: No disponible
MAC: No disponible
Nombres de Servidores
Nombre - Tipo: cotecnova.edu.co - user
Sistema operativo
Nombre: Linux 3.10 - 4.11
Precisión: 94%
Puertos usados
Clases de OS
Secuencia TCP
Filtrar servidores


Aplicaciones
Lugares
Zenmap
dom 11:14
Zenmap
Escaneo Herramientas Perfil Ayuda (H)
Objetivo: cotecnova.edu.co
Perfil:
Escaneo
Cancelar
Comando: nmap -sT -sU -O -v -v -n -Pn cotecnova.edu.co
Servidores
Servicios
Salida Nmap
Puertos / Servidores
Topología
Detalles del servidor
Escaneos
OS
Servidor
cotecnova.edu
Nombre: Linux 3.10 - 4.11
Precisión: 94%
Puertos usados
Puerto-Protocolo-Estado: 21 - tcp - open
Puerto-Protocolo-Estado: 20 - tcp - closed
Clases de OS
Tipo Fabricante Familia OS Generación OS Precisión
general purpose Linux Linux 4.X 94%
Secuencia TCP
Dificultad: Good luck!
Índice: 254
Valores: 44A938EB
Secuencia IP ID
Clase: All zeros
Valores:
Secuencia TCP TS
Clase: other
Valores:
Comentarios
Filtrar servidores

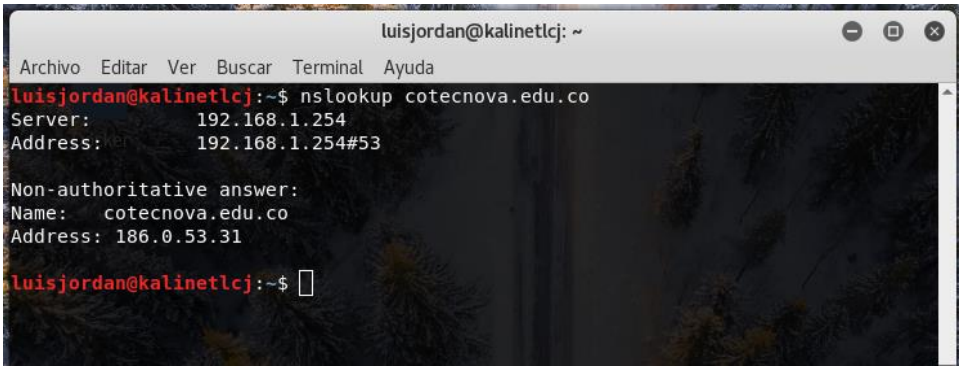


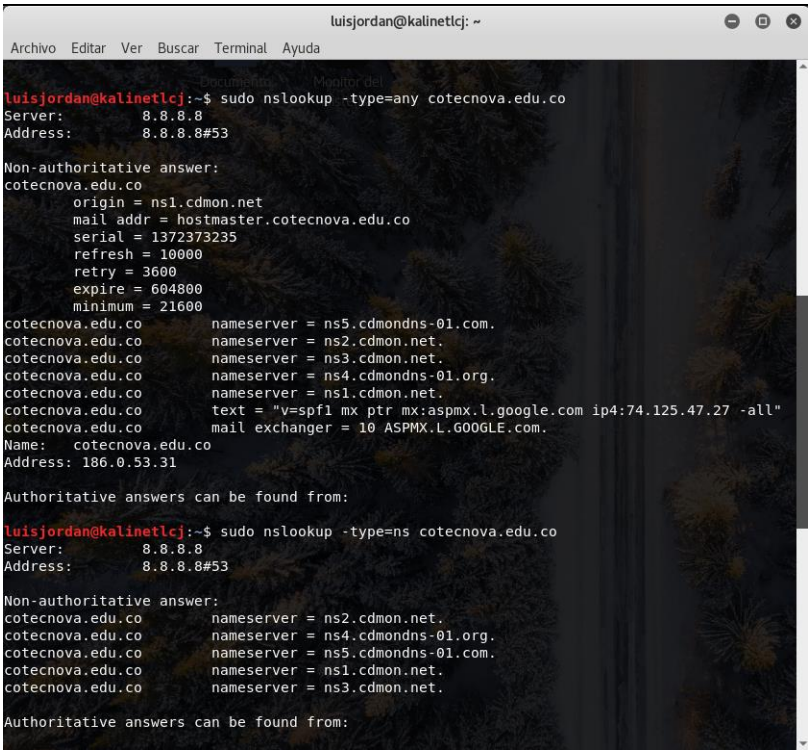
e. Escanee equipos usando NC

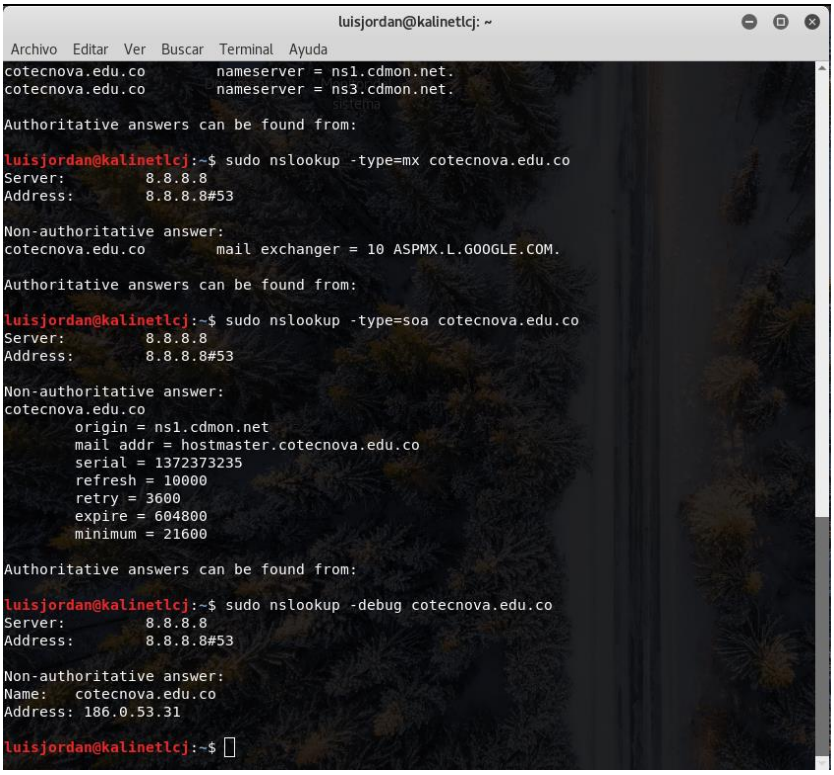




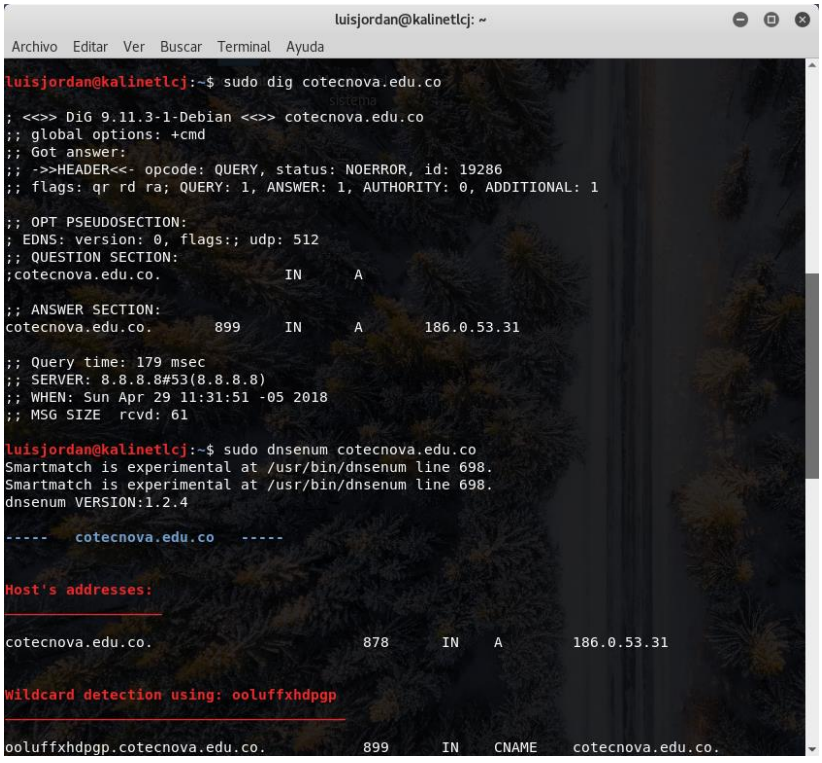
f. Con la herramienta nslookup escanee el dominio cotecnova.edu.co

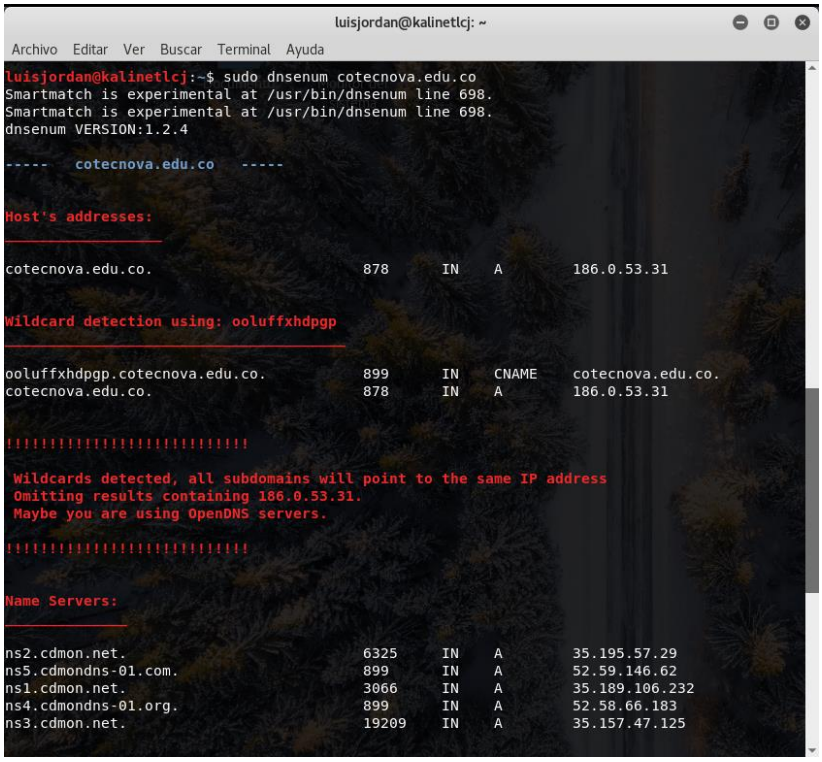


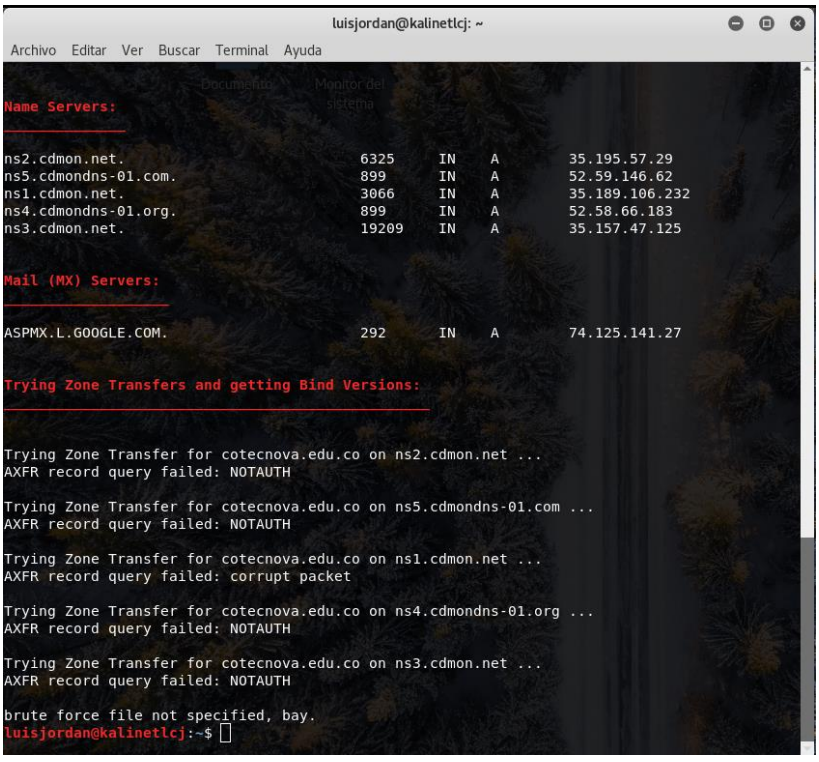




g. Aplicar dig y dnsenum en el dominio cotecnova.edu.co, comparar la información







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 par a 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 que 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.

Recolectad 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 analisis completo al dominio.