

Pràctica 5: Scanners

Infraestructura i Tecnologia de Xarxes

Ramon Guimerà - 1400214
Daniel Morales - 1391627
Grup B10

Respostes:


3.1 Escaneig de la xarxa del dEIC

1. (0.25 punts) Executeu un escaneig de tipus “IP Range” sobre el rang d’IPs 158.109.79.0 a la 158.109.79.255. Trieu 3 màquines que estiguin enceses i no tinguin noms genèrics del tipus deic-número.uab.es.


158.109.79.2	triki.uab.es
158.109.79.4	abra.uab.es
158.109.79.12	macwilliams.uab.es

2. (0.25 punts) Aneu a “Preferences” i modifiqueu les preferències de cerca per tal que Angry IP Scanner trobi algun node que no contesti pings, i algun node amb algun port obert que no sigui ni el 22 ni el 80. Torneu a executar la cerca anterior amb aquests nous criteris. Llisteu un host que tingui obert algun port diferent del 22 i el 80, i algun node que no contesti pings.

El host **deic-dc0.uab.es** te varis ports oberts, però no el 22 ni el 80.

 158.109.79.66	0 ms	deic-dc0.uab.es	7,13,21,111,113,169,859,875,905,931
---	------	-----------------	-------------------------------------

El host **deic-condor-bridge.uab.es** no respon als pings.

 158.109.79.8	[n/a]	deic-condor-bridge.uab.es	[n/s]
--	-------	---------------------------	-------

3.2 Escaneig d'una altra xarxa

1. (0.25 punts) Executeu un escaneig de tipus “Random” sobre el rang d’IPs 158.109.79.0/16. Identifiqueu quatre màquines de departaments/facultats diferents que estiguin enceses.

Algunes de les màquines trobades amb aquest escaneig són les que es poden veure a la imatge:

Scan Go to Commands Favorites Tools Help			
Base IP:	158.109.79.0	IP Mask:	255.255.0.0
Hostname:	deic-dc18	Count	200
Random			
Start			
IP	Ping	Hostname	Ports [0+]
158.109.223.18	0 ms	prn-bibcom-223-18.uab.es	[n/s]
158.109.185.98	1 ms	bibhum-185-98.uab.es	[n/s]
158.109.53.246	44 ms	c2pswtp2-2.uab.es	[n/s]
158.109.223.47	0 ms	bibcom-223-47.uab.es	[n/s]
158.109.64.217	110 ms	q2psw1-6.uab.es	[n/s]
158.109.212.24	0 ms	ibb-212-24.uab.es	[n/s]
158.109.30.247	3 ms	hotswtp2-2.uab.es	[n/s]
158.109.29.248	2 ms	vifnpsw-ap2.uab.es	[n/s]
158.109.215.227	0 ms	platypus.uab.es	[n/s]
158.109.120.89	2 ms	enquestes-mobil-uab-cat.uab.es	[n/s]
158.109.113.141	1 ms	fti-113-141.uab.es	[n/s]
158.109.88.179	2 ms	udvhebron27.uab.es	[n/s]
158.109.224.233	2 ms	dretswtp1-2.uab.es	[n/s]
158.109.201.223	1 ms	[n/a]	[n/s]

2. Executeu un escaneig de tipus “Random” sobre el rang d’IPs 158.109.X.Y/24 on els valors X i Y corresponen a una de les màquines que heu trobat al punt anterior.

S’escolleix com a $X = 215$ i $Y = 227$, que corresponen a platypus.uab.es (marcat a la pregunta anterior en blau). A més a més, a la pregunta 3.2.4 es pot veure que les adreces mostrades en la imatge són del mateix rang.

3. (0.75 punts) Seleccioneu 4 hosts que tinguin obert el port 80. Utilitzeu “botó dret” → “Open” → “Web Browser” per obrir el navegador i intentar connectar-vos a aquestes màquines. Expliqueu a quin tipus de pàgines web us heu connectat (no s’admetran pàgines d’error o de login):

<http://bioinformatica.uab.es/base/base3.asp?sitio=msbioinformatics>

Pàgina web dedicada a un màster en bioinformatica, se presentan los contenidos del curso entre otros aspectos.

<http://mrb-215-113.uab.es/>

Web de la Xarxa de Bancs de Tumors de Catalunya. Informa sobre la xarxa de bancs que hi ha per tota Catalunya, on els professionals que investiguen el càncer poden obtenir mostres pels seus estudis.



























<http://mrb-215-93.uab.es/>

Pàgina web d’una de les impresores que hi ha pel campus. Mostra l’estat del dispositiu i permet canviar la configuració.

<http://mrb-215-58.uab.es/default.asp>

Web de AntiPathoGN, una associació dedicada a l’estudi de bacteries i patògens resistents a diverses drogues.

4. (0.5 punts) Ordeneu els resultats de la cerca per temps de resposta al ping.
Els temps de resposta dels diferents nodes de la mateixa xarxa són similars o veieu algunes diferències significatives?

IP	Ping ^	Hostname	Ports [1+]
 158.109.215.68	0 ms	mrB-215-68.uab.es	80
 158.109.215.131	0 ms	mrB-215-131.uab.es	80
 158.109.215.148	0 ms	mrB-215-148.uab.es	[n/a]
 158.109.215.179	0 ms	mrB-215-179.uab.es	80
 158.109.215.183	0 ms	mrB-215-183.uab.es	[n/a]
 158.109.215.191	0 ms	bioinformatica.uab.es	80
 158.109.215.201	0 ms	mrB-215-201.uab.es	80
 158.109.215.209	0 ms	martini.uab.es	[n/a]
 158.109.215.227	0 ms	platypus.uab.es	80
 158.109.215.14	1 ms	mrB-215-14.uab.es	80
 158.109.215.25	1 ms	mrB-215-25.uab.es	80
 158.109.215.58	1 ms	mrB-215-58.uab.es	80
 158.109.215.88	1 ms	mrB-215-88.uab.es	80
 158.109.215.91	1 ms	mrB-215-91.uab.es	80
 158.109.215.94	1 ms	mrB-215-94.uab.es	80
 158.109.215.102	1 ms	mrB-215-102.uab.es	80
 158.109.215.110	1 ms	mrB-215-110.uab.es	80
 158.109.215.113	1 ms	mrB-215-113.uab.es	80
 158.109.215.125	1 ms	mrB-215-125.uab.es	80
 158.109.215.137	1 ms	mrB-215-137.uab.es	80
 158.109.215.141	1 ms	mrB-215-141.uab.es	[n/a]
 158.109.215.182	1 ms	celler.uab.es	[n/a]
 158.109.215.194	1 ms	embla.uab.es	[n/a]
 158.109.215.214	1 ms	mrB-215-214.uab.es	[n/a]
 158.109.215.244	1 ms	mrbswtp1-5.uab.es	80
 158.109.215.10	2 ms	mrB-215-10.uab.es	80
 158.109.215.121	3 ms	mrB-215-121.uab.es	80
 158.109.215.150	3 ms	mrB-215-150.uab.es	80


Les diferències no son gaire significatives, les màquines que queden més aprop físicament dels laboratoris responen més ràpid.

5. (1 punt) Trieu un host qualsevol d'aquesta xarxa i utilitzeu “botó dret” → “Open” → “Geo-locate” per obtenir les coordenades de la seva ubicació física. Compareu aquesta ubicació amb la que vosaltres suposeu que és la real. Coincideixen? Per què?

General IP Information

IP: 158.109.215.191
Decimal: 2657998783
Hostname: bioinformatica.uab.es
ASN: 13041
ISP: Xarxa Informatica de la
Organization: Xarxa Informatica de la
Services: None detected
Type: [Broadband](#)
Assignment: [Static IP](#)
Blacklist: [Blacklist Check](#)

Geolocation Information

Continent: Europe
Country: Spain 
State/Region: Barcelona
City: Sabadell
Latitude: 41.5433 (41° 32' 35.88" N)
Longitude: 2.1094 (2° 6' 33.84" E)
Postal Code: 08200

Geolocation Map



Segons les coordenades, la màquina es troba a Sabadell. Creiem que no és del tot correcte, ja que si les classes del màster de bioinformàtica s'imparteixen al campus de Bellaterra, el més lògic seria que aquesta màquina es trobi també al campus de Bellaterra. Aquesta diferència es pot deure o a que la màquina realment està a Sabadell o que no es disposa de cap dispositiu d'alta precisió per localitzar geogràficament la màquina, per lo que es fa una aproximació a partir de les dades obtingudes de la adreça IP.

3.3 Una xarxa ja escanejada.

1. (0.5 punts) Des de que en Bob va canviar de despatx, tots els dilluns i dimarts treballa de forma remota des de casa utilitzant SSH en comptes d'anar físicament a la universitat. Quin és el seu nou despatx? Com ho has sabut?

El seu nou despatx es el QC/3041.

La seva màquina es la que te la adreça IP 158.109.79.193, ja que si es mira la informació de NetBIOS d'aquesta màquina es pot veure que a la xarxa es fa dir **WORKGROUP\BOB@QC3041**, es pot veure que es la màquina del Bob i també el seu nou despatx.

2. (0.75 punts) La setmana passada el Bob li va explicar que el nou becari del departament no en sap gaire de xarxes i que, tot i haver instal·lat un servidor web al seu ordinador, era incapaç d'accedir a ell des de casa. Sabries dir quina és la seva adreça IP? Com l'has trobat?

L'adreça de la becaria és la **158.109.79.251**. Si hi ha un servidor web instal·lat, l'Angry IP Scanner es capaç de detectar-ho. Si mirem totes les màquines que tenen un servidor web instal·lat, es pot veure que totes tenen el port 80 obert, excepte la de l'Alba, per això, la becaria no pot accedir des de casa al servidor web.

3. (0.75 punts) En Bob no té gaire clar si els dos estudiants de doctorat del despatx del costat s'han pres un any sabàtic o estan fent feina des de casa, ja que mai els veu al despatx. El que sí que sap és que tenen dues de les tres úniques màquines del departament que utilitzen Windows (l'altra és el servidor de noms). Saps com es diuen aquests estudiants? Atenen-te només a com van configurar les màquines, quin dels dos creus que realment està treballant des de casa i quin creus que pot estar de vacances al Carib?

Les tres màquines que tenen Windows instal·lat són les que tenen les IP 158.109.79.145, 158.109.79.122 i 158.109.79.201. D'aquestes tres, la 122 es pot descartar ja que és el servidor de nom com indica el seu nom NetBIOS.

Les dues màquines restants tenen assignat un hostname (raul.dept.es per la 145 i ivan.dept.es per la 122), amb aquesta informació podem deduir que el estudiants es diuen Raul i Ivan.

Per últim, mirant la configuració es pot suposar que l'estudiant que no està treballant des de casa és l'Ivan, ja que només té el port 53 (DNS) obert i no pot accedir a la seva màquina des de casa. Per altra banda, el Raul té oberts els ports 20 - 22 entre d'altres, aquests són els assignats a FTP i SSH, per tant ell si que pot accedir a la seva màquina des de casa i treballar-hi.

4 - Sessió 2

1. (0.5 punts) Executeu un escaneig de tipus “intense scan” contra venezia.uab.cat. Quins ports té oberts? De què creieu que és servidor?

Escaneig realitzat a venezia.uab.cat:

```
rDNS record for 158.109.168.132: venezia.uab.es
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
25/tcp    open  smtp    Sun Java System Messaging Server smtpd 6.1 HotFix 0.10
| smtp-commands: venezia.uab.es, 8BITMIME, PIPELINING, DSN, ENHANCEDSTATUSCODES, HELP, XLOOP BC586852AEC77DF934D1887FB5424772, STARTTLS, ETRN, SIZE 52428800,
| 2.3.0 Available commands: 2.3.0 2.3.0 DATA, EHLO, EXPN, HELO, HELP, MAIL FROM 2.3.0 NOOP, QUIT, RCPT TO, RSET, SAML FROM 2.3.0 SEND FROM, SOML FROM, TICK, TURN 2.3.0 VERB, VRFY, XADR,
| XSTA, XCIR, ETRN 2.3.0 XGEN, LHLO, AUTH 2.3.0
| ssl-cert: Subject: commonName=*.uab.es/organizationName=Universitat Autònoma de Barcelona/stateOrProvinceName=Barcelona/countryName=ES
| Issuer: commonName=DigiCert SHA2 High Assurance Server CA/organizationName=DigiCert Inc/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Not valid before: 2016-05-10T23:00:00+00:00
| Not valid after: 2019-08-09T11:00:00+00:00
| MD5: 7372 d061 2a0d 4624 263a 235f 79a9 ac8b
| SHA-1: 881b ceel 27e7 0e94 ae6c be03 c654 b71c a49e 5548
| ssl-date: 1970-01-01T05:12:37+00:00; -47y92d6h50m23s from local time.
587/tcp   open  smtp    Sun Java System Messaging Server smtpd 6.1 HotFix 0.10
| smtp-commands: venezia.uab.es, 8BITMIME, PIPELINING, DSN, ENHANCEDSTATUSCODES, HELP, XLOOP BC586852AEC77DF934D1887FB5424772, STARTTLS, AUTH PLAIN LOGIN, AUTH=LOGIN, SIZE 52428800,
| 2.3.0 Available commands: 2.3.0 2.3.0 DATA, EHLO, EXPN, HELO, HELP, MAIL FROM 2.3.0 NOOP, QUIT, RCPT TO, RSET, SAML FROM 2.3.0 SEND FROM, SOML FROM, TICK, TURN 2.3.0 VERB, VRFY, XADR,
| XSTA, XCIR, ETRN 2.3.0 XGEN, LHLO, AUTH 2.3.0
| ssl-cert: Subject: commonName=*.uab.es/organizationName=Universitat Autònoma de Barcelona/stateOrProvinceName=Barcelona/countryName=ES
| Issuer: commonName=DigiCert SHA2 High Assurance Server CA/organizationName=DigiCert Inc/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Not valid before: 2016-05-10T23:00:00+00:00
| Not valid after: 2019-08-09T11:00:00+00:00
| MD5: 7372 d061 2a0d 4624 263a 235f 79a9 ac8b
| SHA-1: 881b ceel 27e7 0e94 ae6c be03 c654 b71c a49e 5548
| ssl-date: 1970-01-01T05:12:37+00:00; -47y92d6h50m23s from local time.
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
```

Com observem en la imatge següent, té oberts els ports 25 i 587.

	Port	Protocol	State	Service	Version
	25	tcp	open	smtp	Sun Java System Messaging Server smtpd 6.1 HotFix 0.10
	587	tcp	open	smtp	Sun Java System Messaging Server smtpd 6.1 HotFix 0.10

El servidor, segons indica l'escaneig, és de pròsit general (Device type), però si anem més a fons, podem veure que són els ports de smtp, per lo que és un servidor de email.

2. (0.5 punts) Executeu un escaneig de tipus “intense scan” contra wiki.uab.cat. Quan acabi, a la pestanya superior seleccioneu “Puertos/anfitriones” i a la columna de l’esquerra seleccioneu wiki.uab.cat com a “Anfitrión”. Veureu que hi ha dos ports diferents oberts catalogats com HTTP. Per què?

Els ports oberts són el 80 i 443, que corresponen als protocols de HTTP i HTTPS respectivament.

Port	Protocol	State	Service	Version
80	tcp	open	http	Apache httpd 2.2.22 ((Debian) PHP/5.3.3-7+squeeze28 with Suhosin-Patch mod_python/3.3.1 Python/2.7.3 mod_ssl/2.2.22 OpenSSL/1.0.1t mod_wsgi/3.3 mod_perl/2.0.4 Perl/v5.10.1)
443	tcp	open	http	Apache httpd 2.2.22 ((Debian) PHP/5.3.3-7+squeeze28 with Suhosin-Patch mod_python/3.3.1 Python/2.7.3 mod_ssl/2.2.22 OpenSSL/1.0.1t mod_wsgi/3.3 mod_perl/2.0.4 Perl/v5.10.1)

Aquests ports estan oberts ja que wiki.uab.cat és una pàgina web (port 80) que utilitza HTTPS (port 443).

3. (0.5 punts) Executeu un escaneig de tipus “intense scan” contra www.uab.cat. Quan acabi, analitzeu la “Salida nmap” i digueu amb quin sistema operatiu funciona www.uab.cat. Esteu segurs d’aquesta resposta? És exacta o aproximada?

Segons l’escaneig i els resultats en la imatge inferior, www.uab.cat pot funcionar amb diferents versions del kernel Linux (no simultànies). Entre aquestes versions es troben: 2.6.32 - 3.10, 3.2 - 3.10, etc.

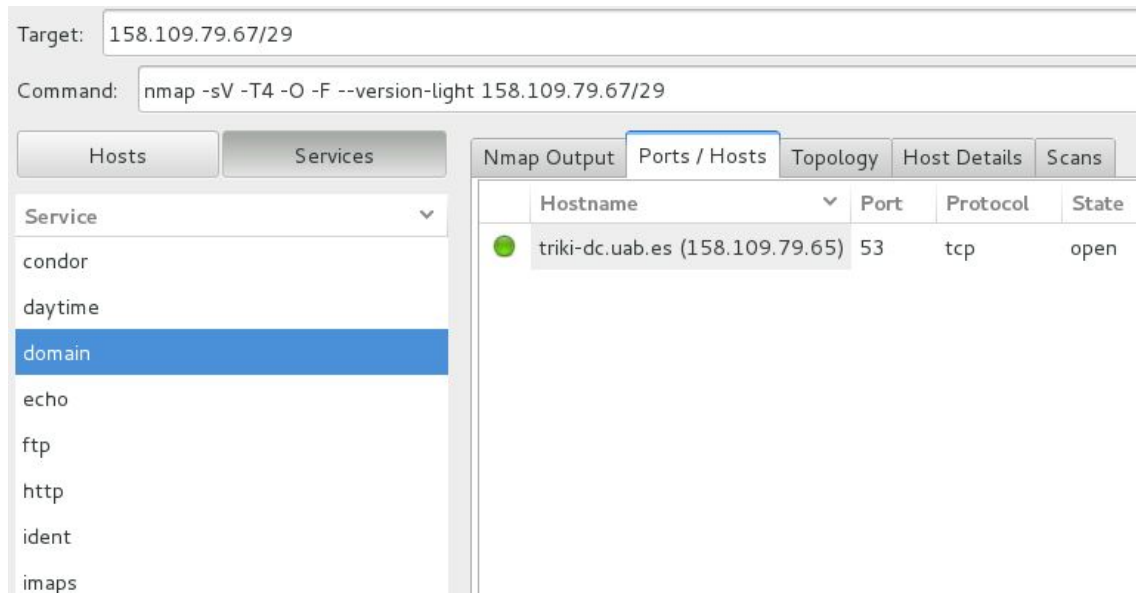
No, no és exacta aquesta resposta, ja que al costat de cada versió possible, hi ha un percentatge que indica el possible encert.

```

Device type: general purpose
Running (JUST GUESSING): Linux 2.6.X|3.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
Aggressive OS guesses: Linux 2.6.32 - 3.10 (91%), Linux 3.2 - 3.10 (90%), Linux 3.2 - 3.8 (89%), Linux 2.6.32 - 3.5 (86%)
No exact OS matches for host (test conditions non-ideal).
```

4. (0.5 punts) Realitzeu un escaneig de tipus “quick scan plus” contra 158.109.79.67/29. Analitzeu la sortida i trobeu quin és el servidor de noms dels equips del laboratori. Com l’heu trobat?

Si anem a la finestra de Services i pestanya de Ports/Hosts podem trobar que domain (DNS) només hi ha un host (triki-dc.uab.es), que és el nostre servidor de noms.



Resultat del quick scan plus:

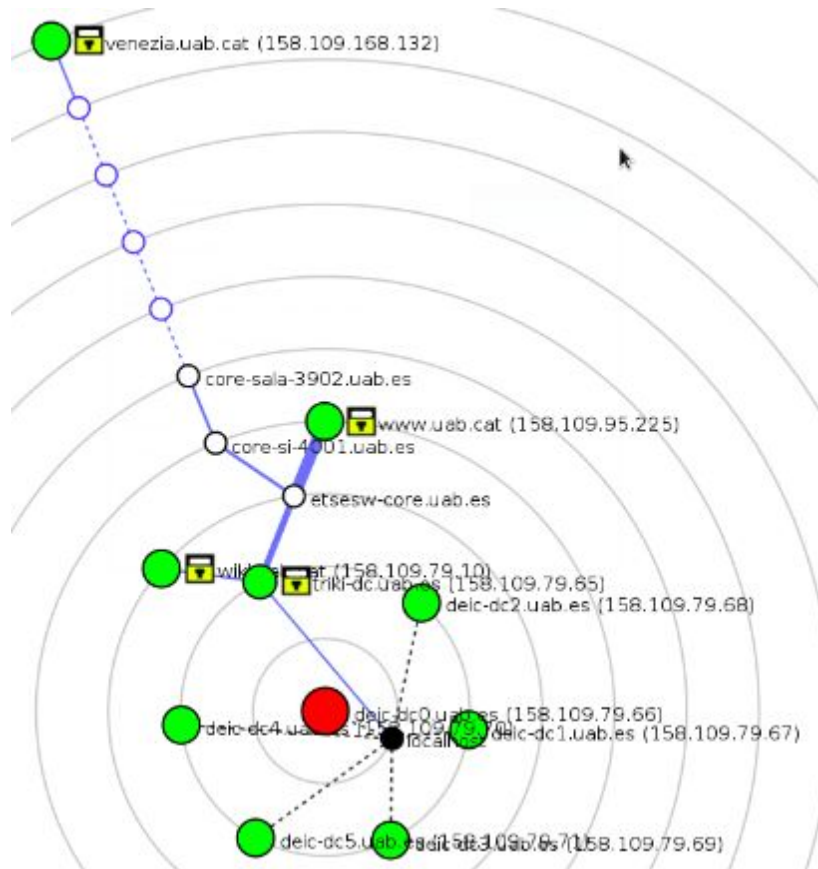
```
Starting Nmap 6.47 ( http://nmap.org ) at 2017-04-03 14:09 CEST
NSOCK ERROR [26.8720s] mksock_bind_addr(): Bind to 0.0.0.0:927 failed (IOD #20): Address already in use (98)
Nmap scan report for triki-dc.uab.es (158.109.79.65)
Host is up (0.00019s latency).
Not shown: 99 filtered ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain
MAC Address: 00:15:17:91:7C:E9 (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10, Linux 3.2 - 3.10
Network Distance: 1 hop
```

5. (0.5 punts) Utilitzeu la pestanya “Salida nmap” per analitzar els resultats produïts per els diferents escaneigs que heu executat. Digueu quines de les següents eines s’han executat durant l’escaneig.

S’han utilitzat les eines de traceroute, nmap i host.

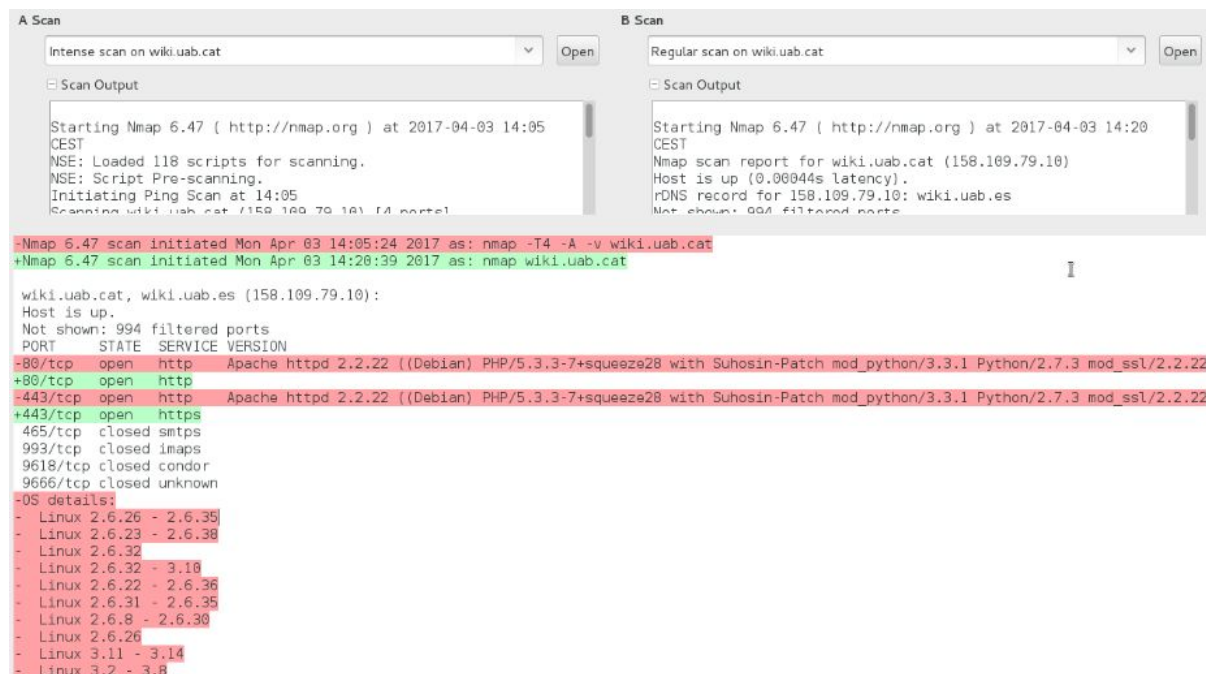
6. (0.5 punts) Utilitzeu la pestanya “Topologia” per consultar el mapa de la xarxa. Amb quina informació Zenmap ha generat aquest mapa? Quines limitacions té aquest sistema?

Utilitza la informació obtinguda al realitzar un traceroute a les diferents màquines per poder fer el mapa de la xarxa. Si hi ha cap firewall que talla el tràfic del traceroute, no es pot generar correctament el mapa.



7. (0.5 punts) Executeu un escaneig de tipus “regular” contra wiki.uab.cat. Utilitzeu l’eina “Comparar resultados” de Zenmap per comparar els resultats d’aquest escaneig amb el que heu realitzat al punt 2. Quines diferències trobeu?

Es pot veure que l’escaneig intens, tal com el seu nom indica, aporta més informació del sistema, com pot ser la versió d’Apache instal·lada o detalls del sistema operatiu.



```
A Scan
Intense scan on wiki.uab.cat
Open

Scan Output
Starting Nmap 6.47 ( http://nmap.org ) at 2017-04-03 14:05
CEST
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 14:05
Scanning wiki.uab.cat (158.109.79.10) [4 ports]

B Scan
Regular scan on wiki.uab.cat
Open

Scan Output
Starting Nmap 6.47 ( http://nmap.org ) at 2017-04-03 14:20
CEST
Nmap scan report for wiki.uab.cat (158.109.79.10)
Host is up (0.00044s latency).
rDNS record for 158.109.79.10: wiki.uab.es
Not shown: 994 filtered ports

-Nmap 6.47 scan initiated Mon Apr 03 14:05:24 2017 as: nmap -T4 -A -v wiki.uab.cat
+Nmap 6.47 scan initiated Mon Apr 03 14:20:39 2017 as: nmap wiki.uab.cat

wiki.uab.cat, wiki.uab.es (158.109.79.10):
Host is up.
Not shown: 994 filtered ports
PORT      STATE SERVICE VERSION
-80/tcp    open  http    Apache httpd 2.2.22 ((Debian) PHP/5.3.3-7+squeeze28 with Suhosin-Patch mod_python/3.3.1 Python/2.7.3 mod_ssl/2.2.22
+80/tcp    open  http
-443/tcp   open  http    Apache httpd 2.2.22 ((Debian) PHP/5.3.3-7+squeeze28 with Suhosin-Patch mod_python/3.3.1 Python/2.7.3 mod_ssl/2.2.22
+443/tcp   open  https
+443/tcp   open  https
465/tcp    closed smtps
993/tcp    closed imap
9618/tcp   closed condor
9666/tcp   closed unknown
-OS details:
- Linux 2.6.26 - 2.6.35
- Linux 2.6.23 - 2.6.38
- Linux 2.6.32
- Linux 2.6.32 - 3.10
- Linux 2.6.22 - 2.6.36
- Linux 2.6.31 - 2.6.35
- Linux 2.6.8 - 2.6.30
- Linux 2.6.26
- Linux 3.11 - 3.14
- Linux 3.2 - 3.8
```

8. (1 punt) Si examineu la informació que heu obtingut al realitzar els “intense scan”, trobareu un camp anomenat “Tiempo funcionando” i un altre anomenat “ Ultimo arranque”. Com ha obtingut Zenmap aquesta informació? Creieu que el valor que us dona és molt fiable?

Per aproximar aquest valor, es basa en la assumpció de que el valor utilitzat pel sistema operatiu per calcular els timestamps utilitzats a TCP es basen en una constant que comença valent 0 al iniciar el sistema i s’incrementa a un ritme constant. El que fa l’eina, és mirar el valor del timestamp de les respostes als diferents SYN que envia. A partir d’aquestes dades calcula la freqüència a la que s’incrementa aquest comptador i calcula quant temps ha passat des de que es va iniciar el sistema ¹.

¹ Uptime guess (online)
<http://nmap.org/book/osdetect-usage.html>

9. (0.5 punts) Si utilitzeu “Topologia” → “Visor de anfitriones” per examinar les dades que heu obtingut sobre wiki.uab.cat, venezia.uab.cat i www.uab.cat, trobareu informació sobre el “TCP sequence index” i un indicador de dificultat. Expliqueu què vol dir i per a què serveix aquest index de dificultat.

Aquest index determina el grau de dificultat per poder predir el següent número de seqüència que utilitzarà TCP. Si resulta molt fàcil calcular el següent número, el sistema està exposat a un atac de *session hijacking* ².

² Session hijacking (online)
<http://www.techrepublic.com/article/tcp-hijacking/>