

3.1. Escaneo de la red del dEIC

1. (1 punto) Plugins Activos. En “Preferences” (botón pequeño al lado de “IP Range”) modifique las preferencias de búsqueda para que Angry IP Scanner encuentre nodos con puertos abiertos del 1 al 100.

De click sobre la columna ping y escoge “Seleccione buscadores”. Agregue todos los Plugins disponibles a Plugins activos. Ejecute un escaneo de tipo “IP Range” sobre el rango IP 158.109.79.0 a 158.109.79.255. Enlista un equipo Apache, nginx, Microsoft-ISS, CentOS, HP, Cisco y 3Com. También enlista un equipo que tenga el puerto 21 filtrado, uno con el puerto 22 filtrado y otro con el puerto 80 filtrado.

Rango de IP: 158.109.79.0 a 158.109.79.255 Rango de IP						
Nombre de equipo: deic-dc3.uab.cat IP ↑ Máscara de red Comenzar						
IP	Ping	Nombre del equipo	Puertos [1000+]	TTL	Puertos Filtrados [1000+]	Detectar Web
158.109.79.3	0 ms	moixero.uab.es	80	[n/a]	1-79,81-442,444-464,466-992,994-1000	Apache
158.109.79.7	0 ms	deic-cluster.uab.es	22,80,175-177,1	[n/a]	1-21,23-79,81-165,178,418-464,466-992,994-1000	Apache/2.2.3 (CentOS)
158.109.79.4	0 ms	abra.uab.es	80,169,443,465,	[n/a]	1-79,81-138,140-168,170-442,444,446-464,466-992,994-1000	Apache/2.4.10 (Debian)
158.109.79.2	0 ms	deic-projectes.uab.es	80,169-171,993	[n/a]	1-79,81-168,172-442,444-464,466-992,994-1000	Apache/2.4.10 (Debian)
158.109.79.3	0 ms	sage.uab.es	80-85,90,91,169	[n/a]	1-20,23-79,87-89,92-168,170-464,466-992,994-1000	Apache/2.4.25 (Debian)
158.109.79.4	0 ms	web-docencia.uab.ca	80,169,443	[n/a]	1-79,81-168,170-442,444-464,466-992,994-1000	Apache/2.4.25 (Debian)
158.109.79.1	0 ms	wiki.uab.es	80,443	[n/a]	1-79,81-442,444-464,466-992,994-1000	Apache/2.4.38 (Debian)
158.109.79.5	0 ms	deic-web.uab.es	80,169,443	[n/a]	1-79,81-168,170-442,444-464,466-992,994-1000	Apache/2.4.38 (Debian)
158.109.79.5	0 ms	dao.uab.es	80,169,443	[n/a]	1-79,81-168,170-442,444-464,466-992,994-1000	Apache/2.4.38 (Debian)
158.109.79.1	0 ms	gici.uab.es	22,80,443	[n/a]	1-21,23-79,81-442,444-464,466-992,994-1000	Apache/2.4.6 (CentOS) Open
158.109.79.1	0 ms	deic-bletchley.uab.es	80,169	[n/a]	1-79,81-168,170-442,444-1000	nginx
158.109.79.1	0 ms	gicilab.uab.es	22,80,443	[n/a]	1-21,23-79,81-442,444-1000	nginx
158.109.79.4	2 ms	pia-79-45.uab.es	443,515,631	[n/a]	80	Virata-EmWeb/R6_2_1
158.109.79.2	0 ms	triki.uab.es	53	[n/a]	1-52,54-1000	[n/a]
158.109.79.2	0 ms	satoshi.uab.es	169	[n/a]	1-79,81-168,170-442,444-464,466-992,994-1000	[n/a]
158.109.79.3	0 ms	[n/a]	22	[n/a]	1-21,23-52,54-79,81-442,444-464,466-992,994-1000	[n/a]
158.109.79.4	0 ms	deic-git.uab.es	169,443	[n/a]	1-168,170-442,444-464,466-992,994-1000	[n/a]

158.109.79.45	1 ms	pia-79-45.uab.es	80,443,515,631	[n/a]	[n/a]	Virata-EmWeb/R6_2_1
158.109.79.1	[n/a]					
158.109.79.2	1 ms					
158.109.79.3	[n/a]					
158.109.79.5	[n/a]					
158.109.79.6	[n/a]					
158.109.79.8	[n/a]					
158.109.79.9	[n/a]					
158.109.79.12	[n/a]					
158.109.79.14	[n/a]					
158.109.79.15	[n/a]					
158.109.79.16	[n/a]					

Apache => check
nginx => check
Microsoft-ISS => No hemos encontrado
CentOS => check
HP => check
Cisco => No hemos encontrado
3Com => No hemos encontrado

puerto 21 filtrado => check
puerto 22 filtrado => check
puerto 80 filtrado => check

2. (0.5 puntos) En “Preferences” (botón pequeño al lado de “IP Range”) modifique las preferencias de búsqueda para que Angry IP Scanner encuentre algún nodo que no responda pings (equipos muertos), y algún nodo con el puerto 993 abierto.

Nodo muerto

Rango de IP:		<input type="text" value="158.109.79.0"/>	a	<input type="text" value="158.109.79.255"/>	<div>Rango de IP</div>	
Nombre de equipo:		<input type="text" value="deic-dc3.uab.cat"/>	<div>IP ↑</div>	<div>Máscara de red</div>	<div>▶ Comenzar</div>	

IP	Ping	Nombre del equipo ▲	Puertos [1+]	TTL	Puertos Filtrados [1+]	Detectar Web	Envío de HTTP	Comentarios	Información
158.109.79.5	[n/a]	abra-mirror.uab.es	[n/a]	[n/a]	933	[n/a]	[n/a]	[n/a]	[n/a]
158.109.79.4	0 ms	abra.uab.es	[n/a]	[n/a]	933	Apache/2.4.10 (Debian)	Sun, 11 Apr 20	[n/a]	[n/a]
158.109.79.49	[n/a]	ariadne.uab.es	[n/a]	[n/a]	933	[n/a]	[n/a]	[n/a]	[n/a]
158.109.79.53	0 ms	dao.uab.es	[n/a]	[n/a]	933	Apache/2.4.38 (Debian)	Sun, 11 Apr 20	[n/a]	[n/a]

Nodo puerto 933 abierto

Rango de IP:		<input type="text" value="158.109.79.0"/>	a	<input type="text" value="158.109.79.255"/>	<div>Rango de IP</div>					
Nombre de equipo:		<input type="text" value="deic-dc3.uab.cat"/>	<div>IP ↑</div>	<div>Máscara de red</div>	<div> Comenzar</div>					
IP	Ping	Nombre del equipo	Puertos [1+]	TTL	Puertos Filtrados [1+]	Detectar Web	Envío de HTTP	Comentarios	Información	Dirección
158.109.79.36	0 ms	moixero.uab.es	[n/a]	[n/a]	933	Apache	Sun, 11 Apr 20	[n/a]	[n/a]	[n/a]
158.109.79.7	0 ms	deic-cluster.uab.es	[n/a]	[n/a]	933	Apache/2.2.3 (CentOS)	Sun, 11 Apr 20	[n/a]	[n/a]	[n/a]
158.109.79.4	0 ms	abra.uab.es	[n/a]	[n/a]	933	Apache/2.4.10 (Debian)	Sun, 11 Apr 20	[n/a]	[n/a]	[n/a]
158.109.79.226	0 ms	deic-projectes.uab.es	[n/a]	[n/a]	933	Apache/2.4.10 (Debian)	Sun, 11 Apr 20	[n/a]	[n/a]	[n/a]
158.109.79.39	0 ms	sage.uab.es	[n/a]	[n/a]	933	Apache/2.4.25 (Debian)	Sun, 11 Apr 20	[n/a]	[n/a]	[n/a]

A partir de ahora, puedes volver a modificar las preferencias de búsqueda a fin de resolver los siguientes ejercicios.

33.2. Escaneo de otra red

1. (0.5 puntos) Ejecute un escaneo de tipo “Random” sobre el rango IP 158.109.79.0/16. Identifique cuatro máquinas de departamentos/facultades diferentes que estén encendidas.

IP	Nombre	Entidad
158.109.52.168	cie-52-168.uab.es	Facultad de Ciencias
158.109.127.14	prn-saf-127-14.uab.es	SAF
158.109.209.181	med-209-181.uab.es	Facultad de Medicina

158.109.111.98	vet-111-98.uab.es	Facultad de Veterinaria
----------------	-------------------	-------------------------

2. (1 punto) Ejecute un escaneo de tipo “Random” sobre el rango IP 158.109.X.0/24 donde el valor de X corresponde a la subred de una de las máquinas que has encontrado en el punto anterior. Luego seleccione 4 hosts que tengan abierto el puerto 80. Finalmente utilice el “botón derecho” -> “Open” -> “Web Browser” para abrir el navegador y conectarse a estas máquinas vía Web(no se admitirán páginas de error o de login):

The screenshot shows the HP LaserJet M402dn web interface in a browser. The address bar shows the URL `saf-127-10.uab.es`. The page title is "HP LaserJet M402dn". The interface includes a navigation menu on the left with options like "Inicio", "Sistema", "Imprimir", "Conexión a red", and "Servicios web HP". The main content area displays the "Estado dispositivo" (Device Status) page. It shows the device is in "Modo de reposo activado" (Sleep mode activated) at IP address 158.109.127.10. Below this, there is a "Resumen de consumibles" (Consumables Summary) section showing the status of the black toner cartridge (Pedir 26X (CF226X)) at 50% capacity. There are also links for "Configuración" (Configuration) and "Gestionar" (Manage) sections.

EPSON TMNet WebConfig \ x +

No es seguro | prn-saf-127-14.uab.es

General Information

Information

- General
- TCP/IP
- SNMP

Configuration

- Network
 - TCP/IP
 - SNMP
 - Community
 - IP Trap 1
 - IP Trap 2
- Option
 - Administrator
 - Password
 - Reset
 - Advanced

EPSON

Online

Administrator Name

Location/Person

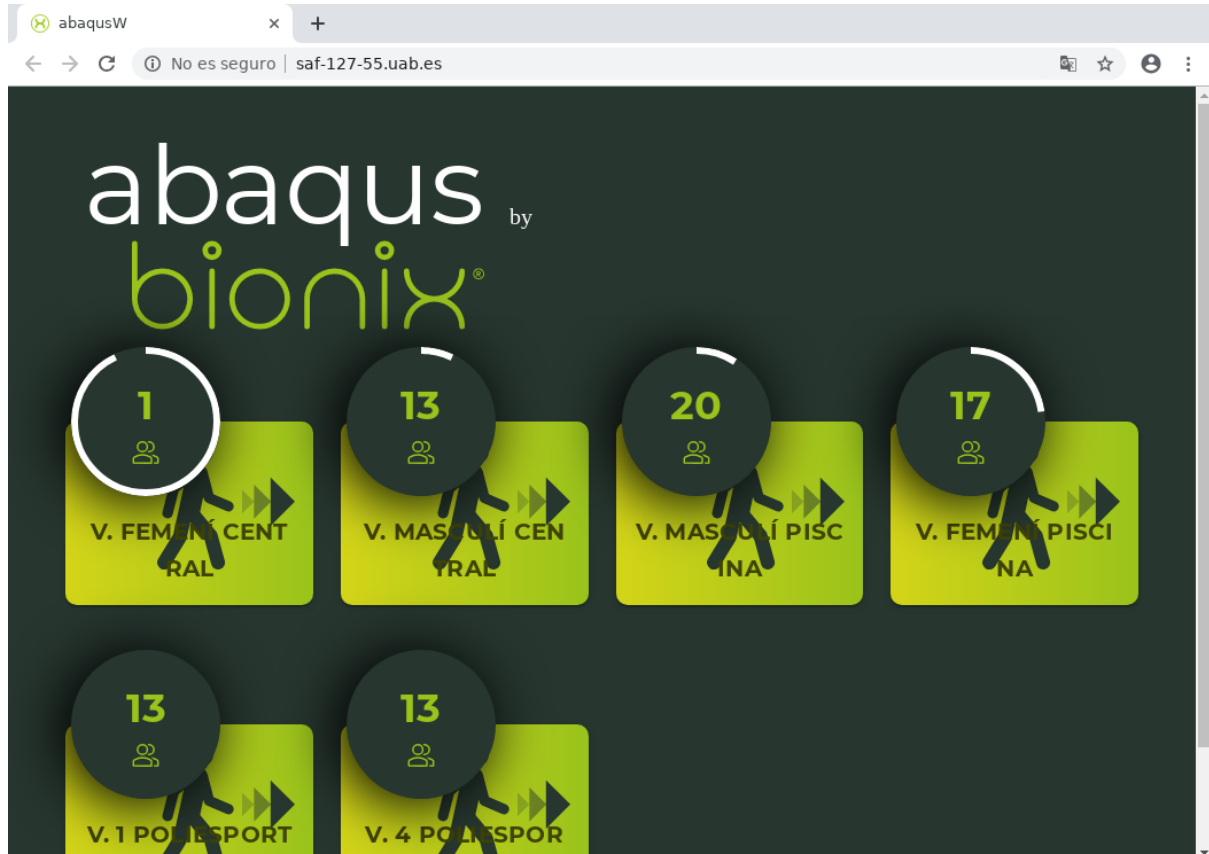
Interface Card

Model Name	UB-E03
MAC Address	64EB8C2C8741
Hardware Version	03.00
Software Version	01.03

Printer

Printer ID	99
Printer Status	Online

Refresh



STS3000 System

No es seguro | saf-127-90.uab.es

STS 3000

Terminal
Terminal Status
Password Setup
Terminal Setup
Communication Setting
Clock Setup

Tools
Device Admin
Reboot
Upgrade Firmware
Diagnostic

Oct.30,2008

TERMINAL STATUS

System Status

Product Name :	STS 3000
Firmware Version :	0.06.00, Feb 11 2009
System Time :	04/19/2021 15:18:09
Terminal ID :	1
Description :	Entrada 2

Serial Port 0 Status

State :	Open
Baud Rate :	9600
Parity Check :	none
Data Bits :	8
Stop Bits :	1

Serial Port 1 Status

State :	Open
Baud Rate :	9600
Parity Check :	none
Data Bits :	8
Stop Bits :	1

Ethernet Status

MAC Address :	00-0e:e3-06-6c:12
IP Address :	158.109.127.90
Subnet mask :	255.255.252.0
Default Gateway :	158.109.124.1
Primary DNS :	168.95.1.1

3. (0.5 puntos) Elige un host cualquiera de esta red y utilice “botón derecho” -> “Open” -> “Geo-locate” para obtener las coordenadas de su ubicación física.

IP Address Lookup for 158. x

https://whatismyipaddress.com/ip/158.109.127.10

WhatIs MyIPAddress.com

Enter Keywords or IP Address... Search

ABOUT PRESS BLOG CONTACT

MY IP IP LOOKUP HIDE MY IP VPNS TOOLS LEARN

Decimal: 2657976074
Hostname: saf-127-10.uab.es
ASN: 13041
ISP: UAB
Organization: Universitat Autònoma de Barcelona
Services: None detected
Type: Corporate
Assignment: Likely Static IP
Continent: Europe
Country: Spain
State/Region: Barcelona
City: Cerdanyola del Vallès

Latitude: 41.4951 (41° 29' 42.36" N)
Longitude: 2.1419 (2° 8' 30.84" E)
Postal Code: 08290

CLICK TO CHECK BLACKLIST STATUS

alternative MPLS
Fast setup, Global coverage, Unlimited bandwidth, Reliable multi-cloud network
Teridion
Learn More >

Privacy

3.3. Una Red ya escaneada

El otro día Alicia utilizó Angry IP Scanner para curiosear la Red de su departamento, pero como aún no ha cursado Infraestructura y Tecnología de Redes, no fue capaz de interpretar los resultados de su escaneo, por eso exportó y cargo en el campus virtual el archivo scan.csv, con la esperanza de que algún alumno con conocimientos suficientes tuviera la capacidad de resolver sus dudas:

a) (0.5 puntos) Desde que Bob cambio de despacho trabaja de forma remota todos los lunes y martes desde casa utilizando SSH en lugar de ir físicamente a la universidad. ¿Cual es su nuevo despacho?

Su nuevo despacho es el QC-3041, porque tiene el puerto 22(SSH) abierto.

b) (0.5 puntos) La semana pasada Bob le explicó que el nuevo becario del departamento no sabe mucho de Redes y que, a pesar de haber instalado un servidor Web en su ordenador, era incapaz de acceder a él desde casa. ¿Cual es la dirección IP del servidor Web?

La dirección ip del servidor es 158.109.79.173, y el motivo por el cual no puede acceder remotamente a él desde casa es porque no tiene abierto el puerto 80.

c) (0.5 puntos) Bob no tiene muy claro si los dos estudiantes de doctorado del despacho vecino han tomado un año sabático o están trabajando desde casa, ya que nunca los ve en el despacho. Lo que se sabe es que tienen dos de las tres únicas máquinas del departamento que utilizan Windows (la otra es el servidor de nombres). ¿Cómo se llaman estos estudiantes? ¿Cual de los dos crees que realmente está trabajando desde casa? y ¿Quién crees que puede estar de vacaciones en el Caribe?

Los estudiantes se llaman Ivan y Raul. El estudiante que está trabajando desde casa es Raul ya que tiene el puerto 23 de telnet abierto y el puerto 3389(TCP que suele usar windows para el escritorio remoto), además del puerto 20, 21 que son los de FTP. El que está de vacaciones en el Caribe es Ivan, ya que no ha dejado ninguno de los puertos ya mencionados abierto para conectarse remotamente.

4. Guión de la práctica: Sesión 2

7. (0.5 puntos) Ejecute un escaneo de tipo “regular” contra wiki.uab.cat. Utilice la herramienta “Comparar Resultados” de Zenmap para comparar los resultados de este escaneo con el que ha realizado en el punto 2. ¿Qué diferencias encuentra?

The screenshot shows the Zenmap interface. At the top, the target is 'wiki.uab.cat' and the profile is 'Regular scan'. The command is 'nmap wiki.uab.cat'. Below this, there are tabs for 'Servidores', 'Servicios', 'Salida Nmap', 'Puertos / Servidores', 'Topología', 'Detalles del servidor', and 'Escaneos'. The 'Servidores' tab is active, showing a list of hosts including 'wiki.uab.cat (158.109.79.10)'. The 'Salida Nmap' tab is also active, displaying the output of the scan. The output shows that the host is up, with a latency of 0.00053s. It lists the open ports: 80/tcp (http), 443/tcp (https), 465/tcp (smtps), 993/tcp (imaps), 9618/tcp (condor), and 9666/tcp (zoomcp). The scan was completed in 16.11 seconds.

Below the main interface, there is a comparison of two scans. 'Escaneo A' is an 'Intense scan en wiki.uab.cat' and 'Escaneo B' is a 'Regular scan en wiki.uab.cat'. The results are displayed in a table format, with the intense scan results in red and the regular scan results in green. The intense scan provides more detailed information, including the version of the service (Apache httpd 2.4.38) and the operating system (Linux 2.6.32 - 3.13).

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Apache httpd 2.4.38
443/tcp	open	https	Apache httpd (SSL-only mode)
465/tcp	closed	smtps	
993/tcp	closed	imaps	
9618/tcp	closed	condor	
9666/tcp	closed	zoomcp	

OS details:

- Linux 2.6.32 - 3.13
- Linux 2.6.22 - 2.6.36
- Linux 2.6.39
- Linux 3.10 - 4.2
- Linux 2.6.32
- Linux 3.2 - 4.6
- Linux 2.6.32 - 3.10
- Linux 3.10
- HP P2000 G3 NAS device
- Linux 2.6.26 - 2.6.35

El intenso scan es todo lo marcado en rojo y el regular todo lo marcado en verde. La diferencia fundamental es que el escaneo intenso te facilita la versión del servicio que se está ejecutando por el puerto, además de detectar la versión del sistema operativo que utiliza el host.

8. (1 punto) Si examina la información que ha obtenido al realizar los “intense scan”, encontrará un campo llamado “Tiempo FUNCIONANDO” y otro llamado “Último arranque”. ¿Cómo ha obtenido Zenmap esta información? ¿Cree que el valor que le da es muy fiable?

Zenmap al detectar el SO del objetivo, usa una opción del protocolo TCP (RFC 1323) que le permite hacer una estimación de hace cuánto tiempo ha sido el último arranque. Aun así, esta estimación puede ser errónea ya que este timestamp puede no haber sido iniciado a 0 en el arranque o puede haber tenido un overflow y no ser preciso.

9. (0.5 puntos) Si utiliza “Topología” -> “Visor de anfitriones” para examinar los datos que ha obtenido sobre wiki.uab.cat, venezia.uab.cat y www.uab.cat, encontrará información sobre el “TCP sequence index” y un indicador de dificultad. Explique que significa y para qué sirve este índice de dificultad.

Algunos SO con una pobre generación de número de secuencia inicial TCP son bastante vulnerables a ataques de spoofing TCP que permitiría al atacante mandar datos desde otra dirección IP y hacernos creer que esta dirección IP está intentando comunicarse con nosotros. Este indicador de dificultad nos indica lo difícil que sería intentar encontrar un algoritmo de generación parecido al del objetivo y obtener el número de secuencia inicial usando un rango como el siguiente: *Trivial joke*, *Easy*, *Medium*, *Formidable*, *Worthy challenge*, *Good luck!*; donde *Trivial joke* sería una dificultad nula hasta *Good luck!* que se consideraría de lo más seguro.