

# Infraestructura y Tecnología de Redes

## Curso 2020-2021

### Práctica 5: *Escáneres de red*

#### Introducción

Hay dos tipos principales de escáneres, los de direcciones IP y los de puertos TCP/UDP. Los escáneres de IP se basan en hacer *ping* a un rango de máquinas para saber si están encendidas o apagadas. Partiendo de esta base, podemos encontrar herramientas más o menos avanzadas que incorporan algunas de las funcionalidades típicas de los escáneres de puertos o que permiten obtener información como el estado de NetBios [1], la dirección MAC de los *hosts*, el grupo de trabajo al que pertenecen, etc.

Por otro lado, los escáneres de puertos son herramientas dedicadas a comprobar si un *host* (habitualmente un servidor) tiene puertos abiertos, y obtener información sobre los mismos. Como ejemplo de casos de uso tenemos dos puntos de vista diferentes:

- Los administradores de red lo utilizan para verificar la seguridad y el cumplimiento de las políticas de seguridad. También lo utilizan para comprobar que los servidores ofrecen los servicios que se espera de ellos, que los *firewalls* filtren los paquetes que deben filtrar, etc.
- Los atacantes utilizan este tipo de herramientas para obtener información sobre posibles objetivos, averiguar qué servicios corren en cada nodo, etc.

#### 1. Herramienta utilizada: Angry IP Scanner

Angry IP Scanner [2] es un escáner de direcciones IP gratuito y multiplataforma escrito en Java diseñado para ser rápido y fácil de usar gracias a su GUI. Dispone de algunas funcionalidades adicionales y permite el uso de *plugins*, exporta los datos obtenidos en diversos formatos y también realiza escaneos de puertos.

Su funcionamiento se basa en tres elementos configurables:

- *Feeders*: Generadores de direcciones a escanear.
- *Fetchers*: Determinan el tipo de información a obtener para cada *host* escaneado.

- *Openers*: Sirven para actuar de forma directa con un nodo escaneado (establecer una sesión SSH o telnet, acceder al servidor Web, etc).

## 2. Herramienta utilizada: Zenmap

Nmap [3] es un escáner de puertos que fue escrito originalmente para Linux con el objetivo de descubrir los *hosts* y los servicios en una red, creando así un “mapa” de esta. Actualmente ha sido llevado a muchas otras plataformas y se distribuye de forma gratuita. Por lo tanto, es uno de los escáneres de puertos más populares del mundo.

Nmap ha ido evolucionando y va mucho más allá de descubrir *hosts* y servicios, hoy en día, se adapta a las condiciones de la red (latencia, congestión), detecta sistemas operativos y versiones de *software* específico de servidores, tiene multitud de modos de escaneo (pensados para esquivar medidas anti-escaneo o para evitar generar alertas en sistemas de detección de intrusiones), permite guardar los resultados en diversidad de formatos, etc.

Zenmap [4] es una interfaz gráfica para sistemas Linux. También es gratuita y está pensada para facilitar el uso de Nmap (se encarga de generar un pedido específico, con una serie de opciones y parámetros en función de cómo queremos que sea nuestra búsqueda) y, sobre todo, para mejorar la extracción de información (navegación por menús, mapas visuales, posibilidad de agrupar o filtrar servicios o *hosts*, etc.).

### 3. Guión de la práctica: Sesión 1

**Todas las respuestas deben ir acompañadas de las gráficas correspondientes que demuestren los resultados de lo que se está explicando, configurando y/o requiriendo.**

Para iniciar Angry IP Scanner, abra una terminal y ejecute `ipscan`.

#### 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 escoja “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. Enliste un equipo Apache, nginx, Microsoft-ISS, CentOS, HP, Cisco y 3Com. También enliste un equipo que tenga el puerto 21 filtrado, uno con el puerto 22 filtrado y otro con el puerto 80 filtrado.



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.



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

### 3.2. 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:
IP:	Nombre:	Entidad:
IP:	Nombre:	Entidad:
IP:	Nombre:	Entidad:

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):

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

### 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 cargó 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 cambió de despacho trabaja de forma remota todos los lunes y martes desde casa utilizando SSH en lugar de ir físicamente a la universidad. ¿Cuál es su nuevo despacho?

- 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, y verificar que el servicio web esta corriendo, era incapaz de acceder a él desde casa. ¿Cuál es la dirección IP del servidor Web?

- 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 sí 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? ¿Cuál de los dos crees que realmente está trabajando desde casa? y ¿Quién crees que puede estar de vacaciones en el Caribe?

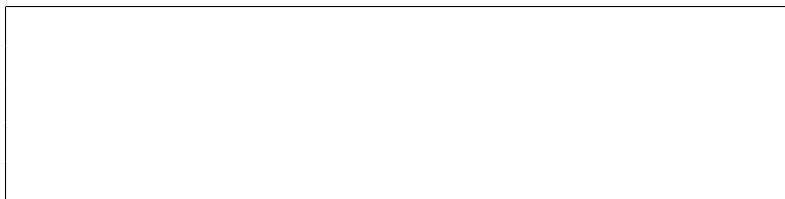
## 4. Guión de la práctica: Sesión 2

**Todas las respuestas deben ir acompañadas de las gráficas correspondientes que demuestren los resultados de lo que se está explicando, configurando y/o requiriendo.**

Para abrir Zenmap, abra una terminal y ejecute `gksudo zenmap`.

**NOTA:** En “Explorar” → “Guardar todos los escaneos en un directorio” podrás guardar todos los datos generados.

1. **(0.5 puntos)** Ejecute un escaneo de tipo “intense scan” contra `venezia.uab.cat`. ¿Qué puertos tiene abiertos?. Basado en los puertos abiertos ¿Qué tipo de servidor es? **(Cuestionario)**



2. **(0.5 puntos)** Ejecute un escaneo de tipo “intense scan” contra `wiki.uab.cat`. Cuando termine, en la pestaña superior seleccione “Puertos/Servidores” y en la columna de la izquierda seleccione `wiki.uab.cat` como “Servidor”. Verá que hay dos puertos diferentes abiertos con versión de servicio Apache httpd. ¿Cuál es la diferencia entre los servicios que se ofrecen por estos dos puertos? **(Cuestionario)**



3. **(0.5 puntos)** Ejecute un escaneo de tipo “intense scan” contra `www.uab.cat`. Cuando termine, analice la “Salida nmap” y diga con qué sistema operativo funciona `www.uab.cat`. ¿Está seguro de esta respuesta? ¿Es exacta o aproximada? **(Cuestionario)**

4. **(0.5 puntos)** Realice un escaneo de tipo “quick scan plus” contra 158.109.79.67/29. Analice la salida y encuentre el servidor de nombres de los equipos del laboratorio. **(Cuestionario)**

5. **(0.5 puntos)** Utilice la pestaña “Salida nmap” para analizar los resultados producidos por los diferentes escaneos que ha ejecutado. Escoja cuáles de las siguientes herramientas se han ejecutado durante el escaneo. **(Cuestionario)**

<input type="checkbox"/> nast	<input type="checkbox"/> traceroute	<input type="checkbox"/> ping	<input type="checkbox"/> who	<input type="checkbox"/> ssh
<input type="checkbox"/> host	<input type="checkbox"/> iptables	<input type="checkbox"/> nmap	<input type="checkbox"/> accés a robots.txt	

6. **(0.5 puntos)** Utilice la pestaña “Topología” para consultar el mapa de la red. ¿Con qué información Zenmap ha generado este mapa? ¿Qué limitaciones tiene este sistema? **(Cuestionario)**

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? **(Informe)**

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? **(Informe)**

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 qué significa y para qué sirve este índice de dificultad. **(Informe)**



## 5. Calendario

A continuación se describe el calendario de los hitos relativos a la práctica:

- **Sesión 1:** El 09/04/2020.
- **Sesión 2:** El 16/04/2020.
- **Entrega:** El 22/04/2020 hasta las 23:55.

## 6. Condiciones de entrega

- La entrega de la práctica se hará a través del campus virtual.
- No se aceptarán informes entregados fuera de plazo.
- Cada grupo debe entregar un informe en formato **PDF que contenga el número de práctica, el número de grupo y el primer apellido de cada alumno** (ej. p1-a1-carpio-miranda.pdf) y las respuestas a los diferentes apartados de la práctica. En caso de **no** seguir el formato se **restará 1 punto de la nota**.

## Referencias

- [1] Wikipedia. NetBIOS. <http://es.wikipedia.org/wiki/NetBIOS>.
- [2] SourceForge. Angry IP Scanner. <http://angryip.org/w/Home>.
- [3] nmap.org. NMAP - Free Security Scanner. <http://nmap.org/>.
- [4] nmap.org. ZENMAP - Official cross-platform NMAP GUI. <http://nmap.org/zenmap/>.