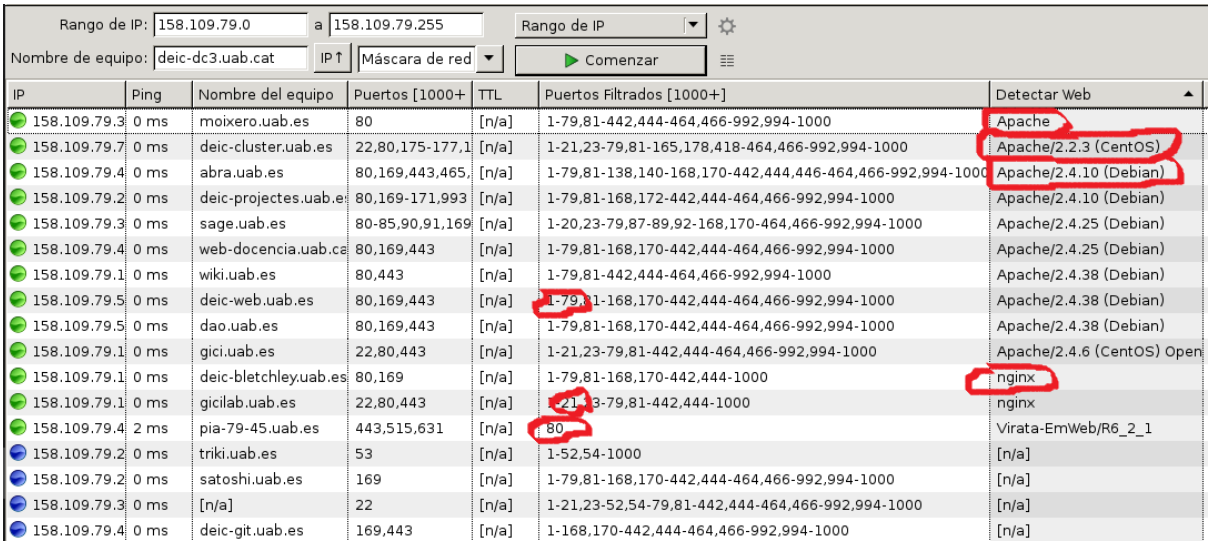
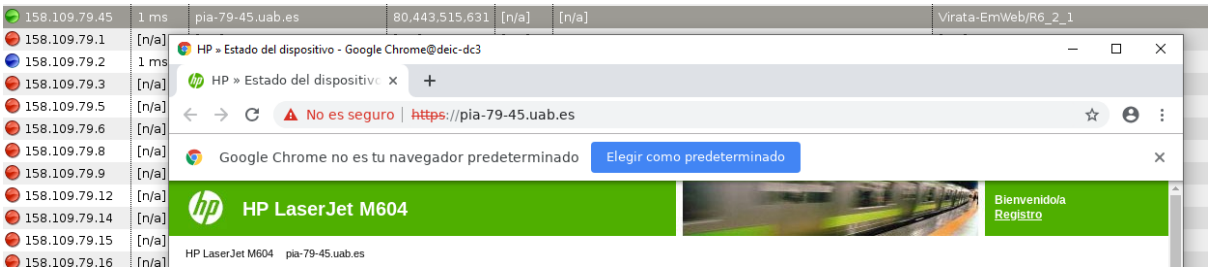
Josep Douton Martin - 1397823
Julio Velásquez Cárdenas - 1397896
Grupo: itx-e3

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.





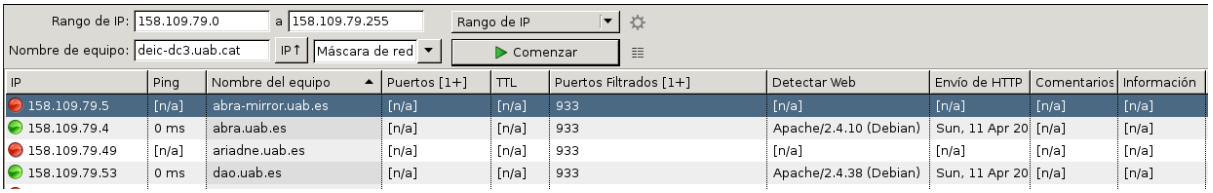
Apache => check
nginx => check
Microsoft-ISS => No hemos encontrado
CentOS => check
HP => check
Cisco => No hemos encontrado
3Com => No hemos encontrado

Josep Douton Martin - 1397823
Julio Velásquez Cárdenas - 1397896
Grupo: itx-e3

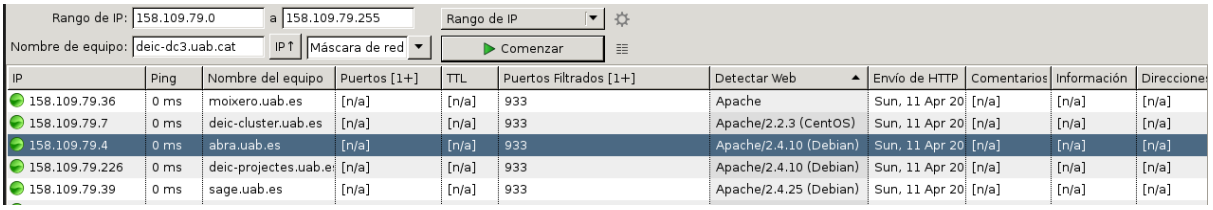
puerto 21 filtrado => check
puerto 22 filtrado => check
puerto 80 filtrado => check

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



Nodo puerto 933 abierto



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

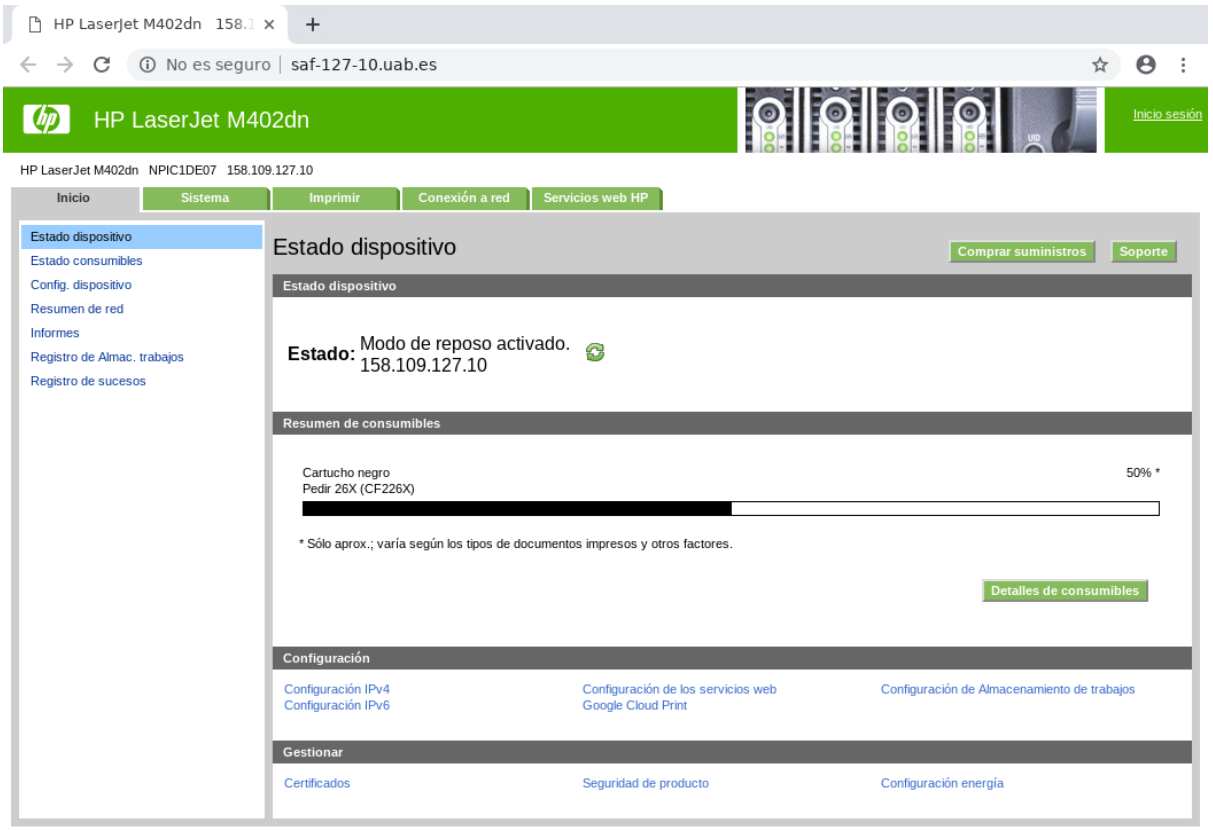
1. (0.5 puntos) Ejecute un escaneo de tipo “Random” sobre el rango IP 158.109.79.0/16. Identifique cuatro máquinas de departamentos/facultades diferentes que estén encendidas.

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

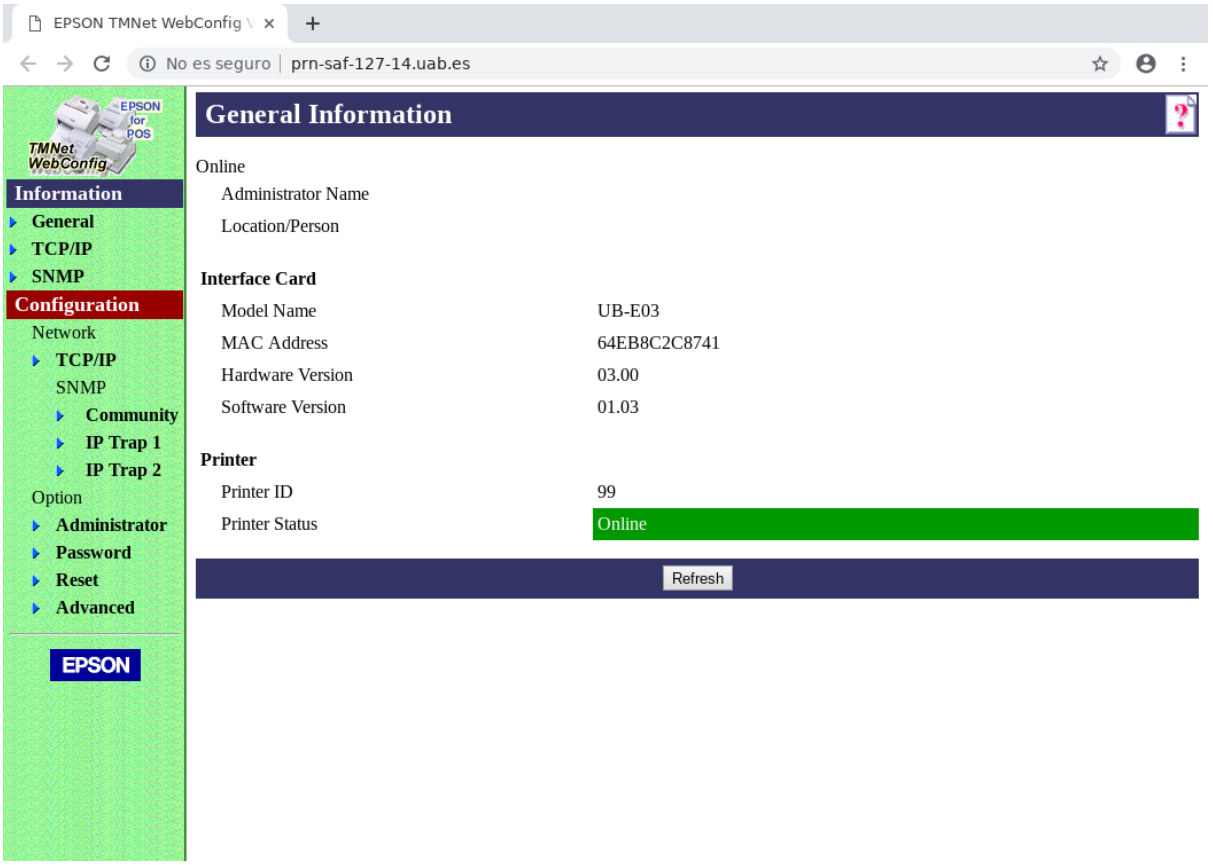
Josep Douton Martin - 1397823
Julio Velásquez Cárdenas - 1397896
Grupo: itx-e3

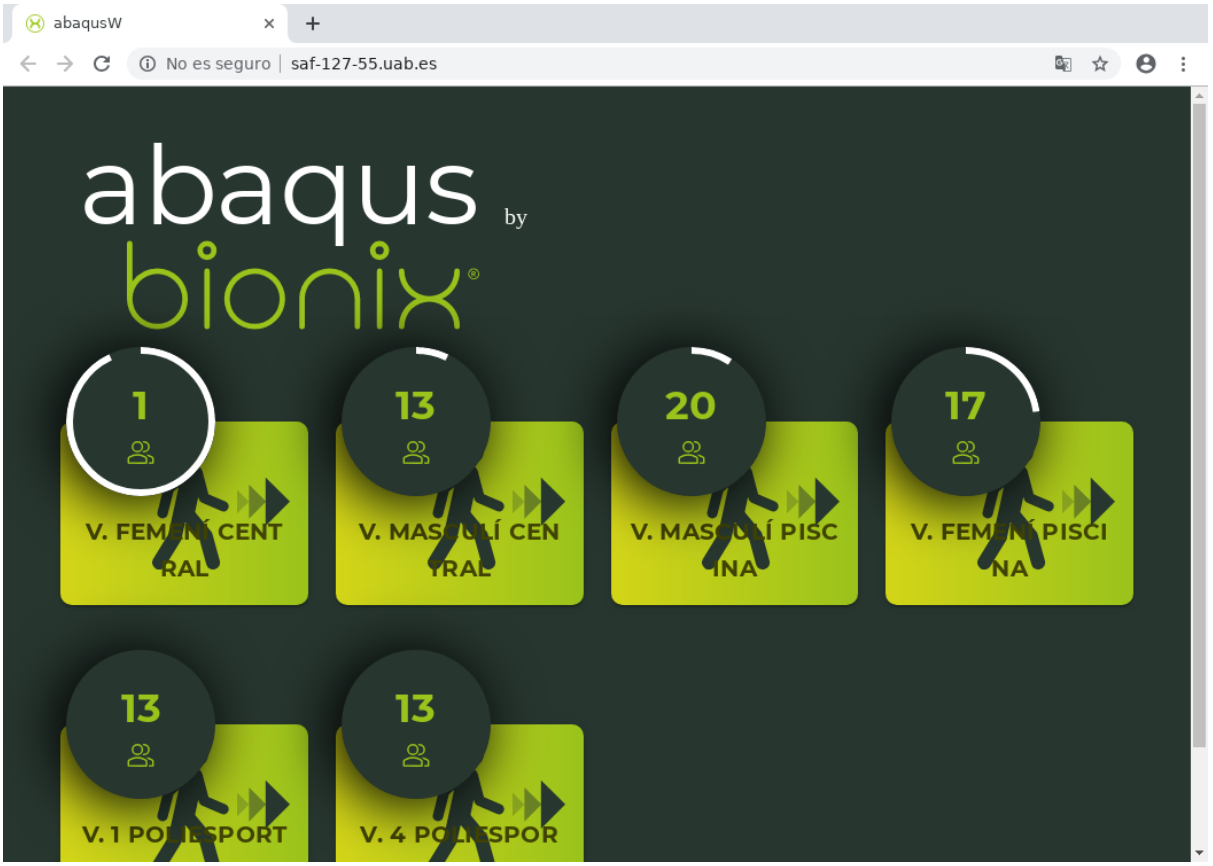
158.109.111.98	vet-111-98.uab.es	Facultad de Veterinaria

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):

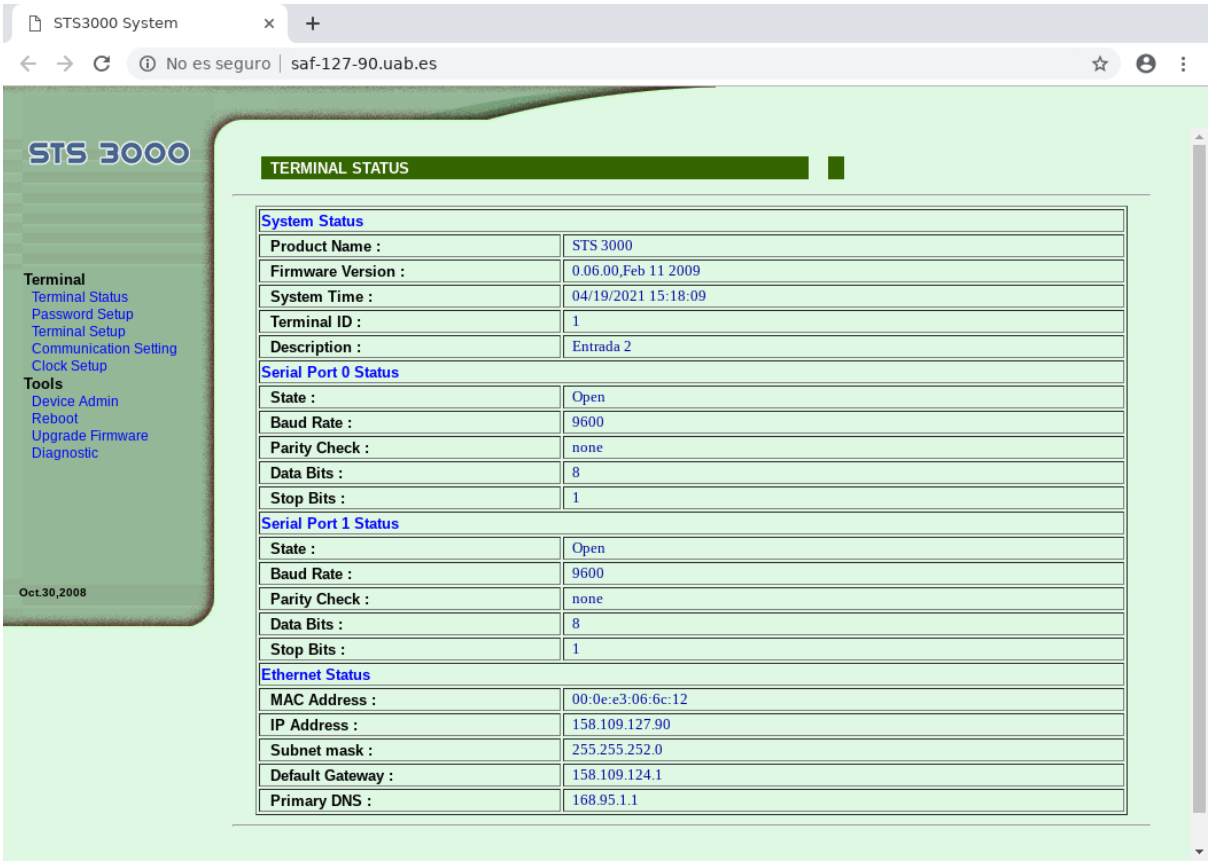


Josep Douton Martin - 1397823
Julio Velásquez Cárdenas - 1397896
Grupo: itx-e3

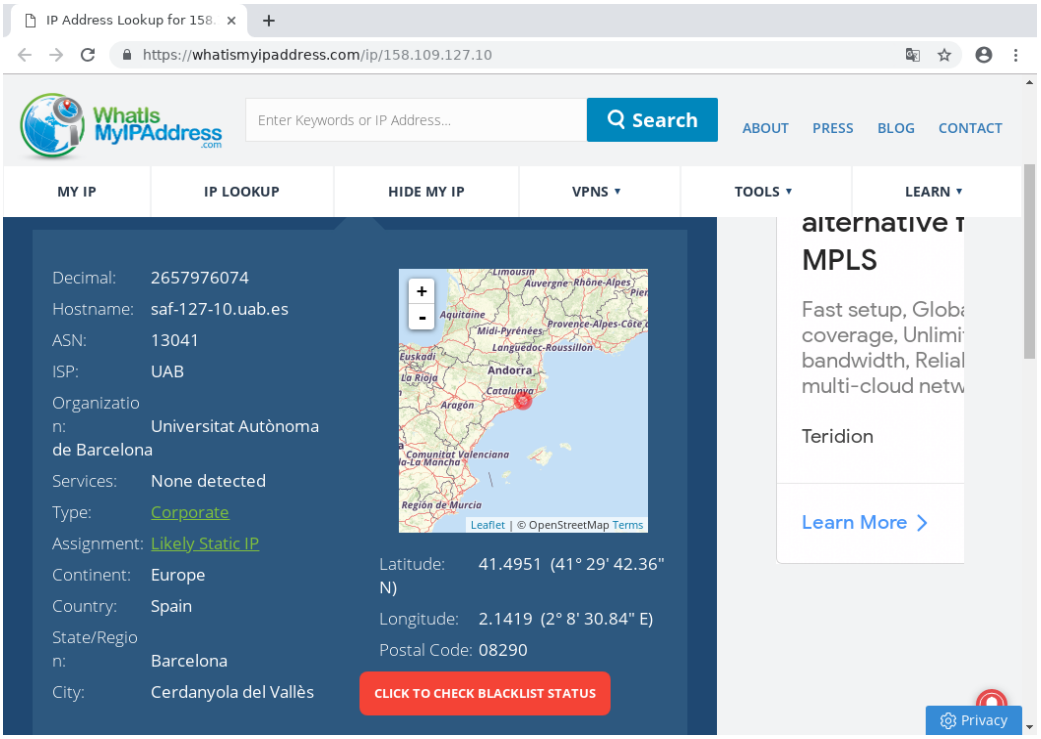




Josep Douton Martin - 1397823
Julio Velásquez Cárdenas - 1397896
Grupo: itx-e3



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.



Josep Douton Martin - 1397823
Julio Velásquez Cárdenas - 1397896
Grupo: itx-e3

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 exporto 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.

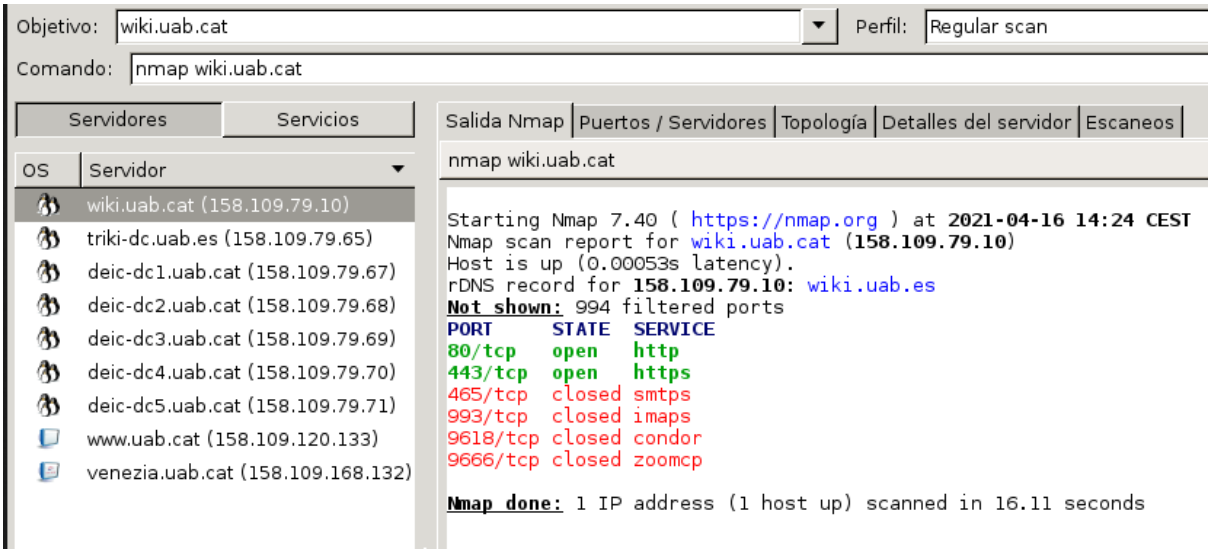
c) (0.5 puntos) Bob no tiene muy claro si los dos estudiantes de doctorado del despacho vecino han tomado un año sabático o están trabajando desde casa, ya que nunca los ve en el despacho. Lo que se sabe es que tienen dos de las tres únicas máquinas del departamento que utilizan Windows (la otra es el 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?

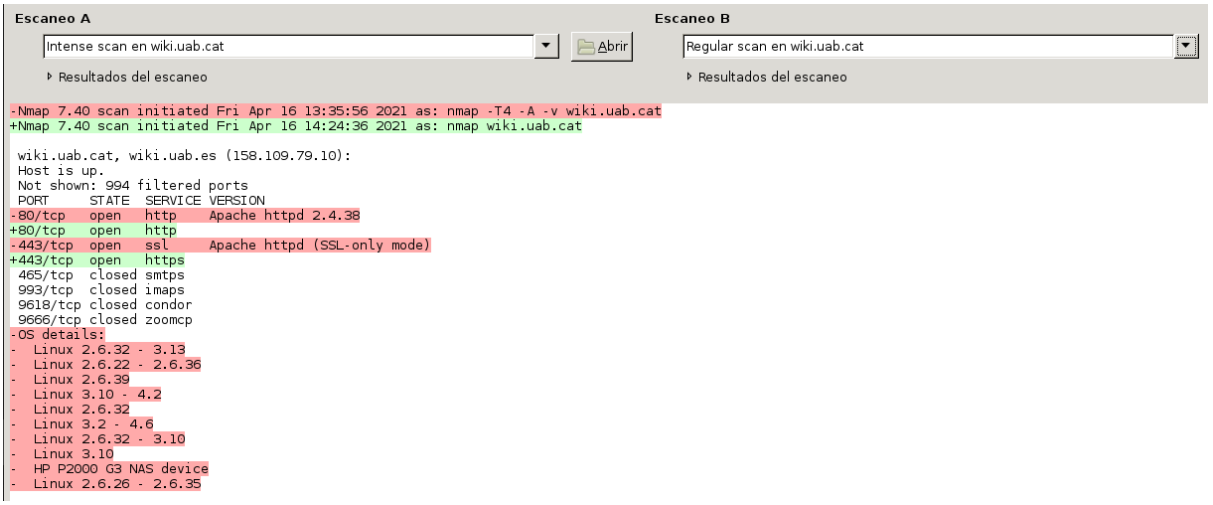
Los estudiantes se llaman Ivan y Raul. El estudiante que está trabajando desde casa es Raul ya que tiene el puerto 23 de telnet abierto y el puerto 3389(TCP que suele usar windows para el escritorio remoto), además del puerto 20, 21 que son los de FTP. El que está de vacaciones en el Caribe es Ivan,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

Josep Douton Martin - 1397823
Julio Velásquez Cárdenas - 1397896
Grupo: itx-e3

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?





El intense 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?

Josep Douton Martin - 1397823
Julio Velásquez Cárdenas - 1397896
Grupo: itx-e3

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.