LABORATORIO 2

Si no sale la dirección buena hacemos un reinicio de la tarjeta de red 🡪 ifup eth0 🡪 ifdown eth0 🡪 ifup eth0

telnet: un servicio que nos permite ejecutar comandos en una maquina remota, desde el punto de vista de hacking permite establecer conexiones TCP con una maquina remota.

ssh: Secure Shell (servicio) se parece mucho al telnet pero telnet toda la información del cliente al servidor la envía sin proteger, mientras que ssh ejecución de comandos de manera segura, si que protege la información y también es un servicio.

Ambos utilizan TCP.

Servicio: WhatsApp, arquitectura cliente-servidor, pueden ser TCP o UDP

Una maquina puede ser un servidor porque atiende las consultas del cliente, y atiende servicios.

1500/TCP – Oracle



1433/TCP – SQL Server

4635/TCP – Correo Electronico

443/TCP – HTTPS

22/TCP – SSH

23/TCP – Telnet

80/TCP – Un servidor WEB

53/UDP – DNS, Query

53/TCP – DNS, Transferencia de Zona

Cuando algo es un servidor para cada uno de los servicios tiene abierto un puerto.

TCP: PROTOCOLO DE CONTROL DE LA TRANSMISION

UDP: PROTOCO DE ALTA DE USUARIOS

-------------- Nslookup ----------------

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Conocer puertos abiertos que tiene una maquina:

Para que un servidor atienda a los clientes ha de tener una dirección IP. Y otra el cliente para poderse comunicar, a parte de la IP en una petición necesitamos a parte de la IP del servidor, necesitamos el puerto para poder utilizar el servicio que yo quiera.

PETICIÓN = (ip\_servidor, puerto)

EMPEZAMOS CON PRÁCTICA

1. Opciones para documentar:

Nmap sirve para mapear la red (descubrimiento de los servicios de un servidor) , es un analizador de puertos.

Cuantos servicios 65035 = 2^16 TCP y 65035 puertos UDP, nmap analiza los 1000 puertos más conocidos

TCP Y UDP son de la capa transporte

-v para que nmap muestre todo lo que esta haciendo cuando hace un descubrimiento de servicios

nmap 10.0.2.4 🡪 de mallet a alice, esto ha analizado 990 puertos (por defecto), se han descubierto los servicios de los 1000 servicios TCP, más utilizados, los servicios UDP con un escaneo por defecto no se muestran (usa TCP)

Texto

Descripción generada automáticamente

El resto no han sido escaneados.

Parámetros para decirle a nmap que analice todos 🡪 nmap 10.0.2.4 -p-

Texto

Descripción generada automáticamente

nmap 10.0.2.4 -p- -v 🡪 únicamente analiza TCP

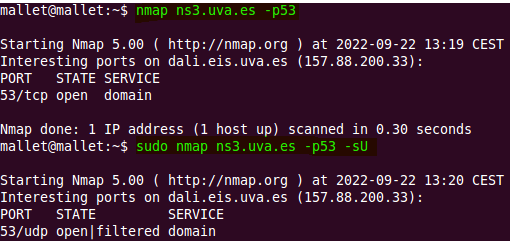
Texto

Descripción generada automáticamente

sudo nmap 10.0.2.4 -p- -sU 🡪 escanea los UDP, tarda mas

nmap ns3.uva.es -p53 🡪 escanea el puerto 53 pero TCP

nmap ns3.uva.es -p53 -sU 🡪 escanea el puerto 53 pero UDP



nmap ns3.uva.es -p53 -sU -sT 🡪 escanea el puerto 53 TCP (-sT) y UDP (-sU)

-sT de tipo TCP completo

-sS también para el protoco TCP, de tipo SYnt

La diferencia entre SYnt y TCP completo es que:

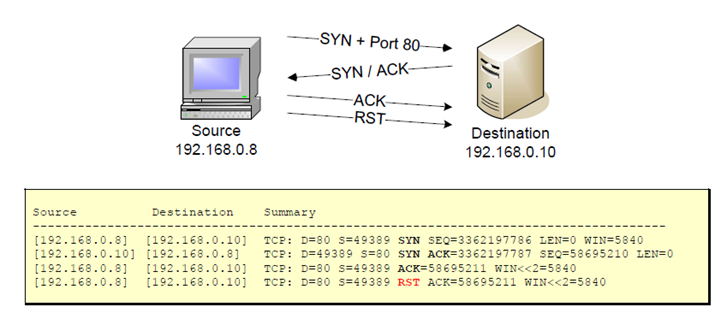
-sT 🡪 El cliente envía un SYN, para sincronizarse con el servidor, y envía un numero de secuencia para ello y el Servidor envía otro SYN, envía un ACK (mensaje de confirmación positivo), es el número de secuencia del cliente +1.

-sS 🡪 basta con que le llegue el SYN + ACK no necesita más, (escaneo sigiloso)

Texto

Descripción generada automáticamente

-sT : (foto de Toribio) 🡪 Esquema clase



Diagrama

Descripción generada automáticamente

-n: le dice a nmap que no intente adivinar el nombre completamente cualificado de la maquina que no haga resolución inversa de DNS.

-sN: no escanea todos los puertos.

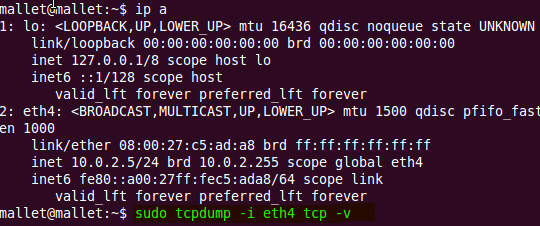
(INVESTIGAR ALGUNO MÁS)

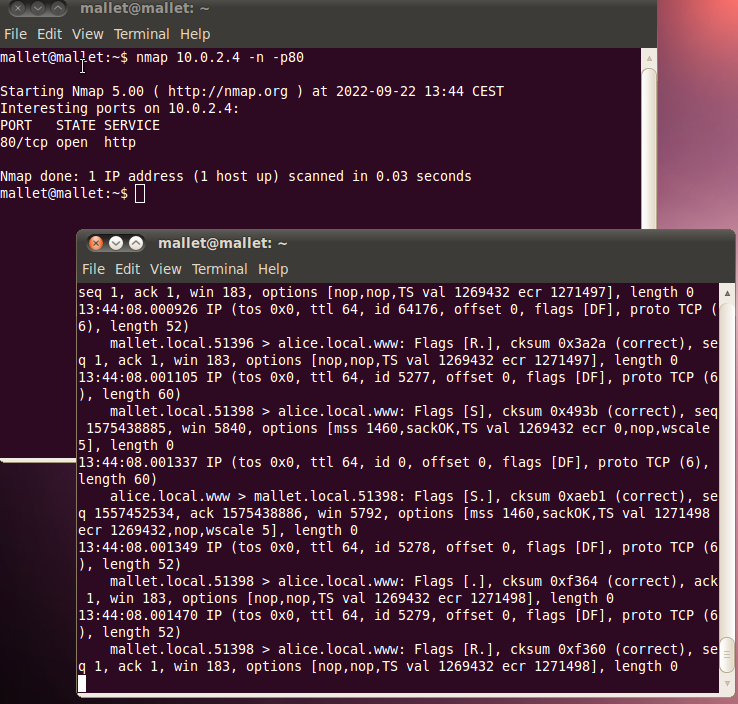
RESPUESTA A A) Y C)

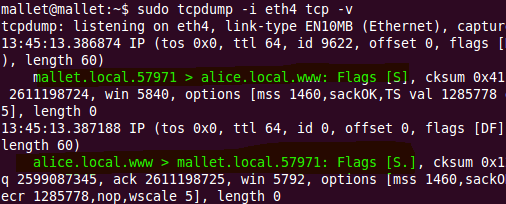
Monotorizacion TCP 🡪 TCP DUMP

Analizador de trafico de red b) :

Con -i le dices cual es la interfaz de red para que lo analice y solo protocolo TCP







Sudo tcpdump -i eth4 tcp -v port 80(-e mas información)

Ahora con escaneo sigiloso

Texto

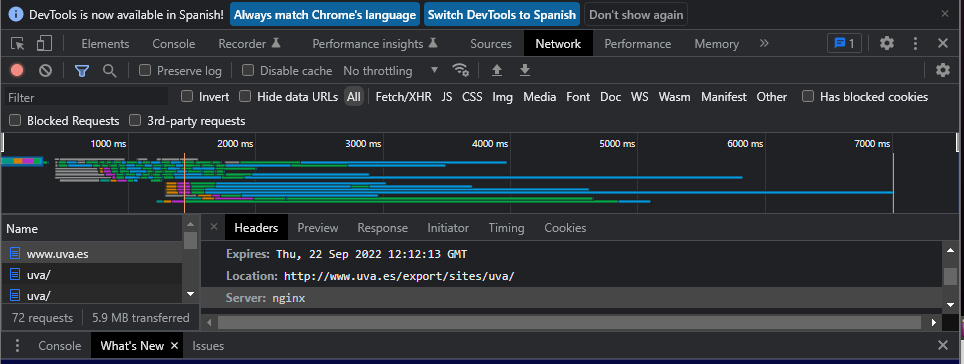
Descripción generada automáticamente

El escáner:



[S.] el . es un +ACK

Nmap [www.uva.es](http://www.uva.es) –p80 -sV (ves la versión del servicio)



Para la d)

Texto

Descripción generada automáticamente

Apache/2.2.14

Vulnerabilidades???

Texto

Descripción generada automáticamente

Exploit-db para ver las vulnerabilidades