Tema 5 tarea 3

**Ejercicio 1: captura de una sesión HTTP con Wireshark**

# Para realizar el ejercicio, el entorno NETinVM debe activarse mediante la realización de las siguientes acciones:

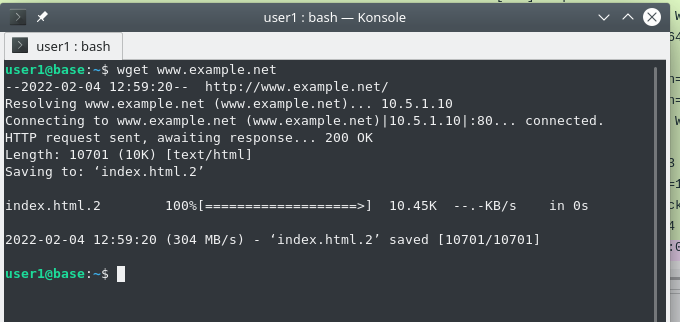
Inicie la máquina virtual de VMware "NETinVM"

# Inicie, dentro de "NETinVM", las máquinas virtuales KVM (Kernel Virtual Machines) ejecutando en "base", como usuario "user1", el comando "netinvm\_run\_all" (o bien, utilice el botón "Run all").

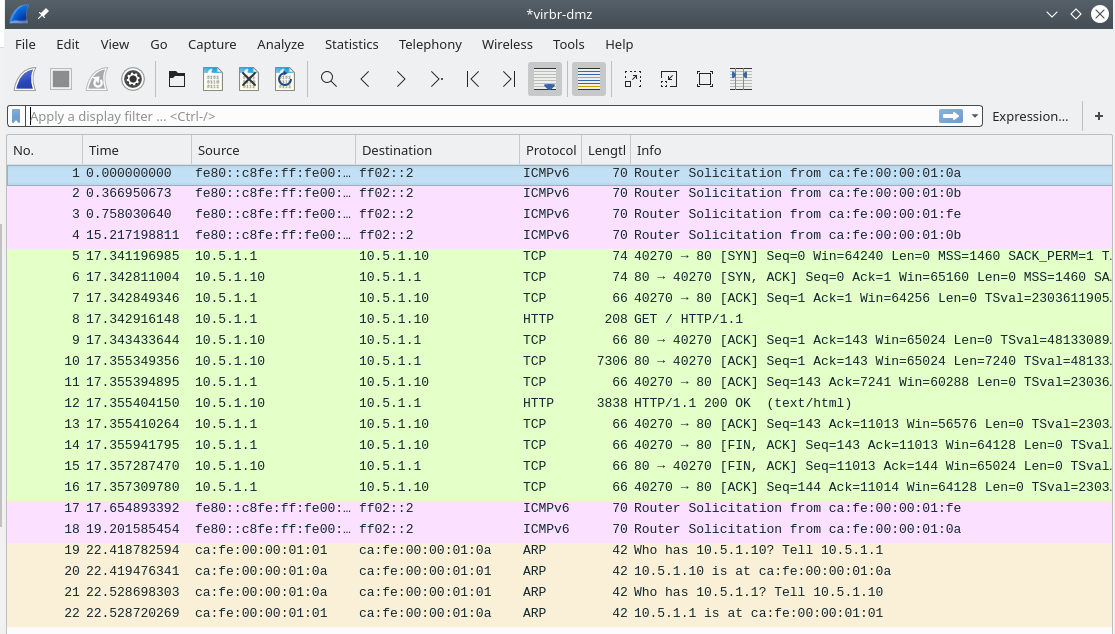
Inicializar la captura de wireshark



Obtener la pagina [www.example.net](http://www.example.net)



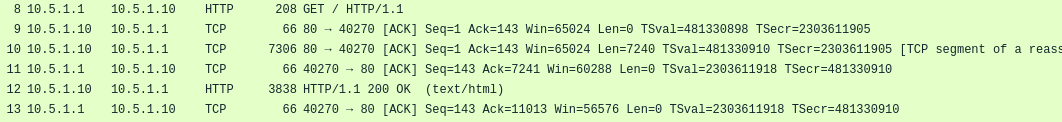
Analizar los paquetes



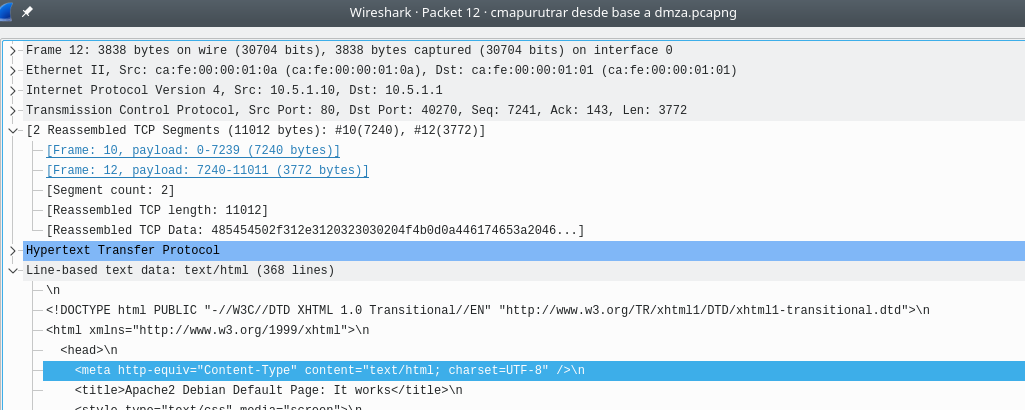
Podemos encontrar paquetes SYN ACK que son paquetes que se encargan de inicializar la comunicación entre el servidor y el cliente.



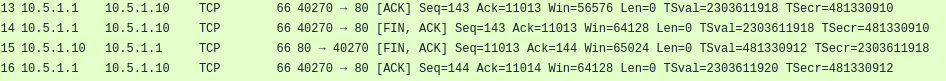
Después paquetes tenemos más paquetes ACK y paquetes HTTP que son los que llevan el HTML de la pagina web, los paquetes ACK se encargan de validar los traspasos de información, por ejemplo cuando el servidor manda el paquete HTTP con la pagina, el cliente debe mandar un paquete ACK de vuelta al servidor para confirmar el recibimiento de la pagina.



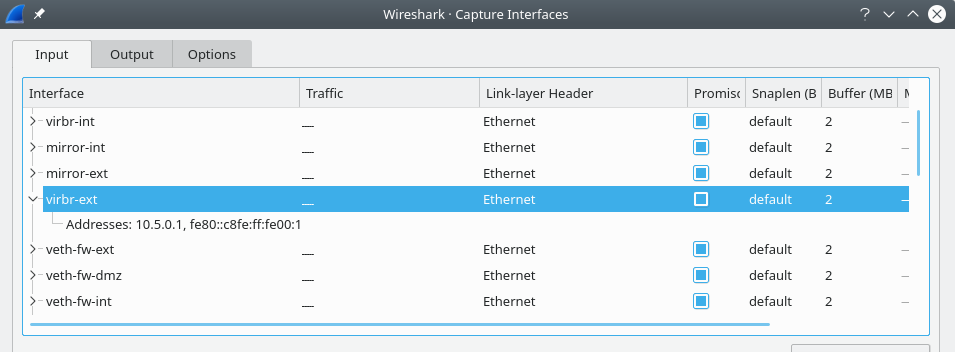
Dentro del paquete HTTP podemos ver el propio código HTML de la pagina



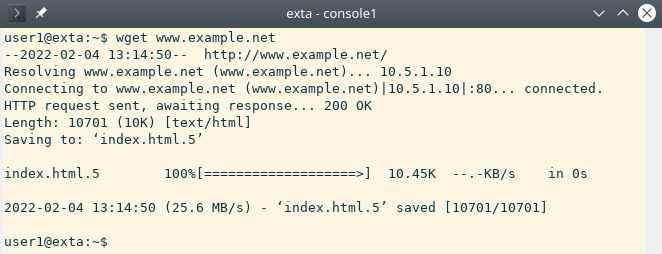
Y después tenemos los paquetes FIN ACK que son paquetes de finalización de la comunicación



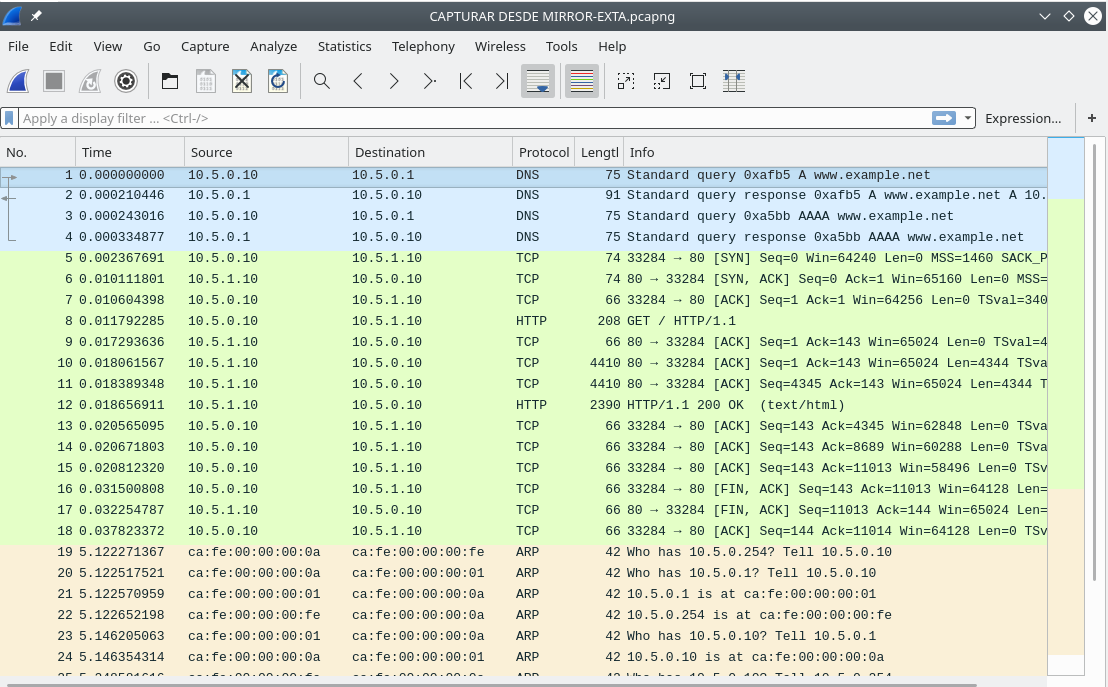
Capturar los paquetes desde exta



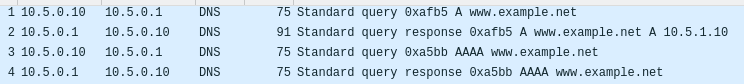
Obtener la pagina



Analizamos los paquetes



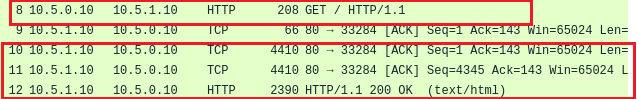
En un inicio podemos ver trafico DNS que trata de resolver el nombre de [www.example.net](http://www.example.net) a la IP de la maquina DMZA



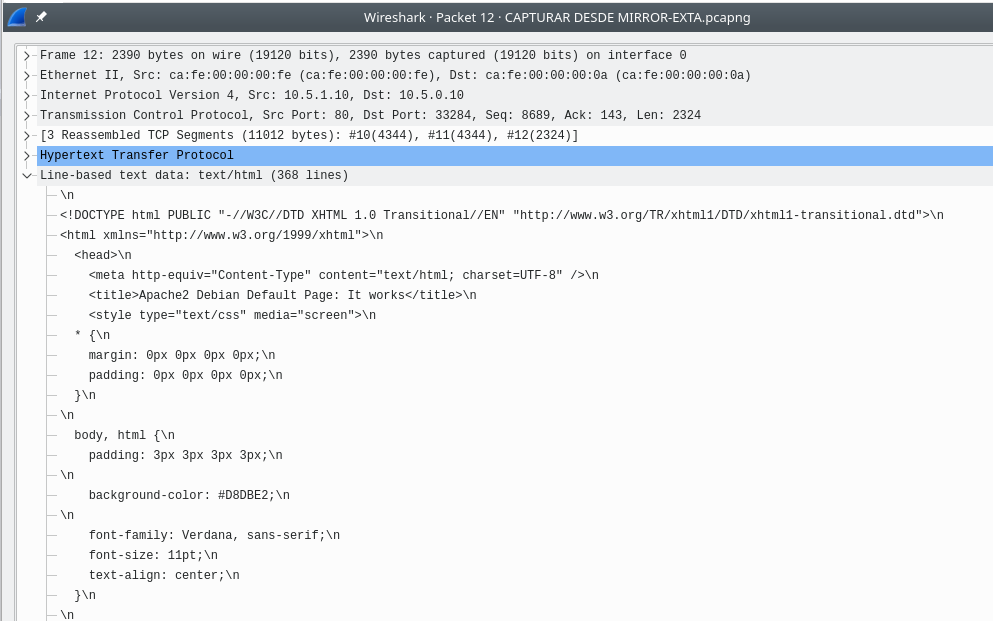
Después encontramos paquetes de sincronización de ACK para iniciar la comunicacion



Después tenemos diferentes paquetes ACK y los paquetes que llevan la propia página web, aquí podemos encontrar 1 paquete “GET” que hacer una request para la pagina web, y después tenemos 3 paquetes, 2 que son “TCP segment” y 1 HTTP , los “TCP segment” son partes de la pagina web



Este es un paquete HTML que lleva parte de la pagina



Después tenemos otros paquetes ACK que sirven como validación de la conexión



Y por ultimo tenemos paquetes FIN ACK, que sirven para finalizar la comunicación



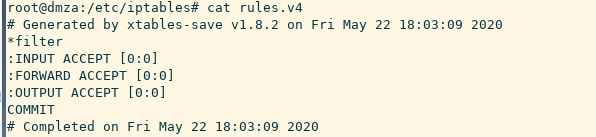
**Ejercicio 2- Configuración de cortafuegos perimetral**

# 2º) Convertir los cambios realizados en persistentes. Usando comandos de iptables.

Lo primero de todo saber que el fichero en el que se almacenan las reglan de iptables es : **/etc/iptables**

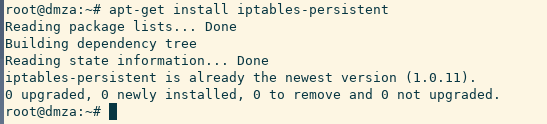
****

Aquí veremos que nos aparece las reglas de ipv4 e ipv6



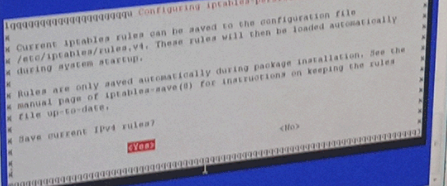
Para llevar el ejercicio a cabo deberemos de instalar el siguiente paquete:

apt-get install iptables-persistent



Lo que nos permite hacer este comando es mantener la configuración de reglas de iptables luego de un apagado o reinicio de la máquina.

Una vez terminada la instalación se nos abrirá una interfaz la cual nos va a permitir guardar las reglas actuales que tienes en iptables



Usaremos los siguiente comandos para controlar el programa:

service iptables-persistent start

service iptables-persistent stop

service iptables-persistent force-stop

service iptables-persistent restart

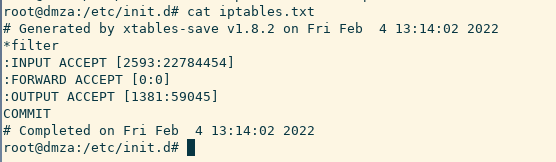
service iptables-persistent force-reload

service iptables-persistent status

una vez hecho esto podremos ver el contenido de el archivo de configuración también con el comando iptables-save :



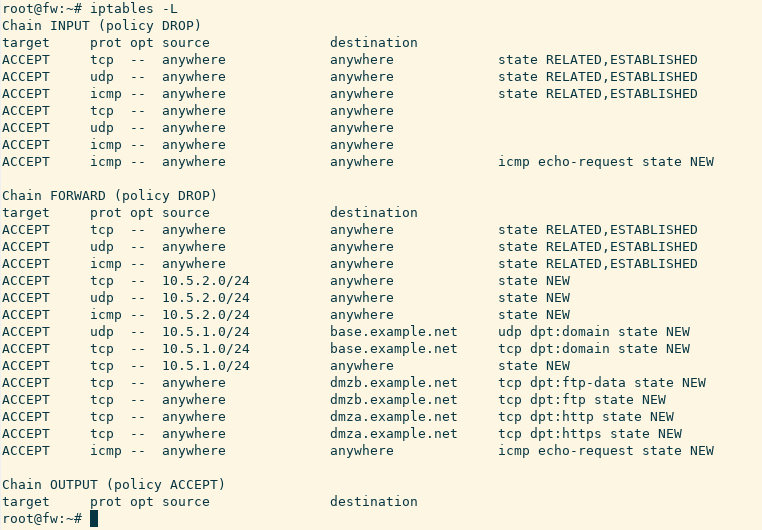
Ahora haremos un cat de ese archivo:



Este archivo lo usaremos como copia de seguridad, ya que con el comando iptables-restore podemos restaurar los valores guardados en iptables desde la copia de seguridad:



3º Analizar las reglas existentes en el fw, proporcionándolas un enunciado, tras agruparlas.



INPUT:



Esta regla permite la entrada en el equipo de cualquier origen y destino de los paquetes tcp, de los equipos con conexión ya establecida.



Esta regla permite la entrada en el equipo local de cualquier origen y destino de los paquetes udp, de los equipos con conexión ya establecida.



Esta regla permite la entrada en el equipo local de cualquier origen y destino de los paquetes icmp, de los equipos con conexión ya establecida.



Esta regla permite la entrada en el equipo local de cualquier origen y destino de los paquetes tcp, de los equipos con la conexión no establecida.



Esta regla permite la entrada en el equipo local de cualquier origen y destino de los paquetes udp, de los equipos con la conexión no establecida.



Esta regla permite la entrada en el equipo local de cualquier origen y destino de los paquetes icmp, de los equipos con la conexión no establecida.



Esta regla permite la entrada en el equipo local de cualquier origen y destino de los paquetes icmp, todos los ping normales que realizamos en clase.

Forward:



Estas reglas permiten los paquetes que pasan a través de nuestro equipo de cualquier origen y destino de los paquetes tcp, udp y icmp, de los equipos con conexión ya establecida.



Estas reglas permiten los paquetes que pasan a través de nuestro equipo de la red 10.5.2.0/24 hacia cualquier destino de los paquetes tcp, udp y icmp, de las conexiones con estado nuevo.



Estas reglas permiten los paquetes que pasan a través de nuestro equipo de la red 10.5.1.0/24 hacia base.example.net de los paquetes tcp y udp, de las conexiones con estado nuevo.



Estas reglas permiten los paquetes que pasan a través de nuestro equipo de la red 10.5.1.0/24 hacia cualquier destino de los paquetes tcp, de las conexiones con estado nuevo.



Estas reglas permiten los paquetes que pasan a través de nuestro equipo de cualquier origen hacia el dmzb.example.net de los paquetes tcp, de las conexiones ftp con el usuario dpt mediante los puertos 20 y 21.



Estas reglas permiten los paquetes que pasan a través de nuestro equipo de cualquier origen hacia el dmzb.example.net de los paquetes tcp, de las conexiones http y https con el usuario dpt mediante los puertos 80(http) y 443(https).



Esta regla permite los paquetes que pasan a través de nuestro equipo de cualquier origen hacia cualquier destino icmp, todos los ping normales que realizamos en clase.

.