INFORME PRACTICA 2

Nombre y apellidos:

ESTA PRÁCTICA SE DEBE REALIZAR EN LOS ORDENADORES DEL LABORATORIO

PARTE 1: PRIMEROS PASOS CON WIRESHARK

Cuestión 1: Experimenta con algunos filtros:

dns Aparecen los paquetes pertenecientes al protocolo DNS
ip.src == XXX.XXX.XXX.XXX (pon tu IP) Saca los datos de los paquetes cuya fuente es tu IP
*ip.dst == XXX.XXX.XXX.XXX (pon la IP del servidor de la página web de la EHU/UPV) * Saca los datos cuyo destino sea esa IP*
*http.host == www.google.com **

** Seguramente, al aplicar esto filtros no se muestre ningún paquete. ¿Por qué? No olvides que para poder ver los paquetes de una conexión tiene que existir dicha conexión, es decir, se debe abrir la página web, por ejemplo.*
No aparece nada porque no hemos enviado ningún paquete.

Utiliza el comando de red *ipconfig* para conocer la IP de tu PC y la puerta de enlace predeterminada. ¿Cómo puedes conocer la IP del servidor EHU/UPV? ¿Que nos permiten ver nuestro analizador con los filtros anteriores?

Nslookup www.ehu.eus

Cuestión 2: Define los filtros que:

- Presenten los paquetes cuya dirección IP de origen sea *host1* y su dirección IP de destino sea la *host2* (o viceversa, dos filtros diferentes)
  ip.src == XXX (Nuestra IP) && ip.dst == YYY (Otra IP)
  ip.src == YYY (Otra IP) && ip.dst == XXX (Nuestra IP)

- Capturar todo el tráfico cuyo origen y destino es el host *host1* y el host *host2*, o host *host2* y el host *host1*, respectivamente (un único filtro)
  (ip.src == XXX (Nuestra IP) || ip.src == YYY (Otra IP)) && (ip.dst == YYY (Otra IP) || ip.src == XXX (Nuestra IP))

- Visualiza todo el tráfico menos el *host1*

ip.src != XXX && ip.dst !=XXX (XXX=al IP del host1)

*como *host1* y *host2* elige tu dirección y la de otro ordenador del aula.

Cuestión 3: Analiza la información y realiza una representación esquemática. ¿Es lo mismo que podíamos ver en la simulación con Packet Tracer?

Vemos que nos mandan 1 paquete, respondemos, mandan el 2º paquete, respondemos, mandan el 3º paquete, respondemos, mandan el 4º paquete, respondemos.

Vemos que mandamos 1 paquete, nos responden……

Vemos lo mismo que en Packet Tracer.

Cuestión 4: Permite que se vean todos los paquetes. ¿Aparecen algún paquete del **protocolo ARP**? Analiza la información de este paquete e intentan explicar cuál es la funcionalidad de este protocolo.

No aparece ninguno entre nuestros dos ordenadores, pero sí si miramos sin filtros. El destino de los protocolos ARP siempre será broadcast.

La funcionalidad de ese protocolo es encontrar la dirección física a través de una dirección IP.

PARTE 2: ANALIZANDO PROTOCOLOS CON WIRESHARK

Cuestión 5: Analiza la captura realizada y explica cómo funciona el comando tracert (recuerda utilizar filtros)

Siempre tendremos una de las dos direcciones IP en el Source o el Destination. De vez en cuando perderemos algún paquete, porque el tiempo de respuesta es muy largo.
El comando tracert rastrea la ruta que sigue un paquete de datos desde tu computadora hasta un destino específico, mostrando todos los nodos intermedios que atraviesa en el camino

Cuestión 6: Analiza los paquetes del protocolo **DNS** que aparecen justo antes de los paquetes anteriores. ¿Qué función crees que tiene este protocolo? ¿Cuál es la dirección de tu servidor DNS? Describe un mensaje DNS (response), desglosando cada cabecera existente en él (y los campos más significativos de cada cabecera).

El protocolo DNS proporciona una dirección IP para cada nombre de host y enumera los servidores de intercambio de correo para cada dominio.
Mi dirección de mi servidor DNS es 212.142.173.65, se puede ver es ipconfig en cmd.
Un mensaje DNS tiene 4 cabeceras:
1)Header/Cabecera: indica cómo se debe manejar y procesar el mensaje(contiene un bit que indica si la pregunta se responde o no).
2)Question/Pregunta: pregunta al servidor. Todos los mensajes DNS debentener una pregunta (y solo una).
3)Answer/Respuesta: esto contiene el registro de recursos (RR). Puede tener una sola respuesta o muchos RR.
4)Authority/Autoridad y **Additional/Adicional:** pueden contener exceso deinformación o pueden estar vacíos