Universidad de Buenos Aires
Facultad de Ingeniería

Seguridad en Redes
TP – Análisis de Protocolos

1. Objetivo

Analizar el funcionamiento de protocolos de capa de aplicación en base a la utilización de los clientes de los mismos y realizando capturas de frames en la red.

2. Prerrequisito

Verifique el correcto funcionamiento de la red en su host así como la dirección IP del mismo. Recuerde que los clientes de los procolos estudiados tienen un help al cual se accede generalemente ingresando un ? y que también existe el comando man.

3. Capturas

FTP

1. Se inicia la captura en el servidor.
2. Transfiera un archivo de texto desde su host hasta el servidor.
3. Verifique que el archivo haya sido transferido mediante un listado del contenido del directorio.
4. Renombre el archivo que acaba de transferir en el servidor.
5. Cierre la sesión y espere a que termine la captura.

HTTP

1. Iniciar servidor WEB apache en nodo1
2. Se inicia la captura de trafico
3. Desde nodo 2 acceder a una pagina del nodo 1. (ver IP en el anexo)
4. Finalizar captura del trafico

Ping

1. Iniciar la captura de trafico
2. Desde nodo 2 hacer ping al nodo 1.
3. esperar unos segundos y finalizar captura

SSH

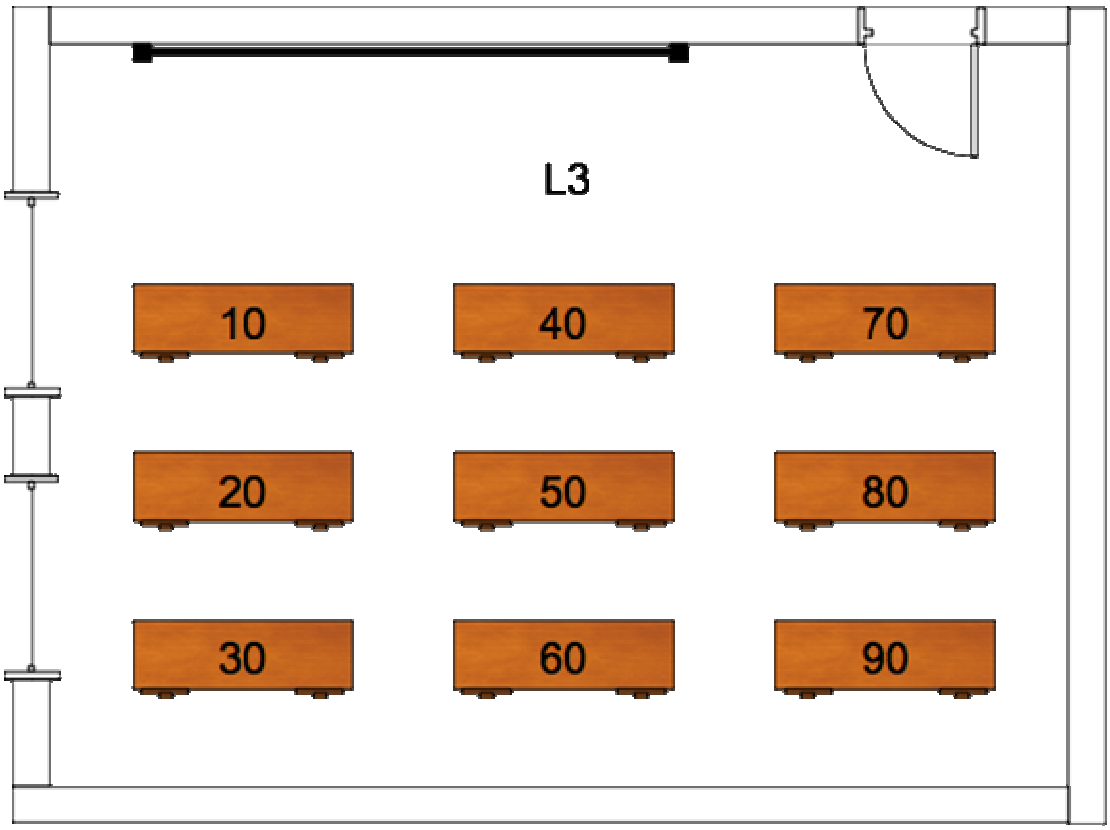
4. Iniciar la captura de trafico
5. Desde nodo 2 hacer ssh al nodo 2 con la opcion -vvv.
6. ejecutar ls / en nodo remoto
7. salir de la conexion
8. Finalizar captura

4. Análisis de las trazas

1. Verificar las Mac address de las trazas con la de cada nodo involucrado.
2. Analizar las capturas: Puertos, Conexiones, Origen, Destino.
3. Parámetros Principales del TCP:
    a. Inicio de la conexión.
    b. Fin de la conexión.
4. Ver el dialogo utilizando la opcion “follow TCP Stream”
5. Describir los protocolos ftp y http.
6. Comparar http con icmp (ping).
7. Que tipo de protocolo es icmp y como esta encapsulado.
8. Ver el dialogo de ssh utilizando la opcion “follow TCP Stream”
9. comparar la captura con la salida del comando ssh -vvv

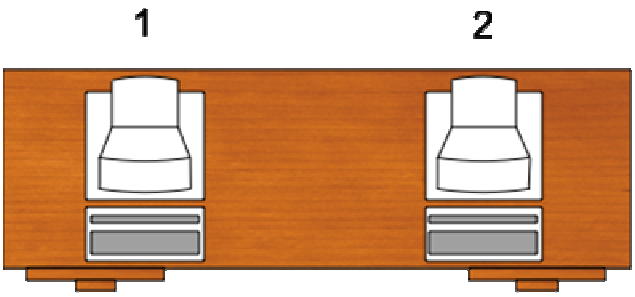
5. ANEXO: Asignación de IP de placas de red

192.168.X.Y donde X es



(se muestra la distribución de mesas en el aula L3)

e Y es



(la distribución de maquinas en cada mesa de la L3)