



Trabajo Práctico de Integración de Conocimientos

Configuración de Redes y Análisis de protocolos

Este trabajo práctico final tiene como objetivo principal la integración de los contenidos teóricos de la asignatura con las habilidades adquiridas durante las clases de laboratorio aplicándolos a un caso de estudio real que puede ocurrir en su vida profesional. Se plantea una topología de red junto con una serie de consignas a resolver.

La actividad propuesta se divide en dos partes: en la primera, deberán configurar dispositivos y servicios de acuerdo a las especificaciones. Esta tarea se realizará colaborativamente en el aula, con el equipo docente coordinando las acciones. La segunda parte corresponde a la generación de tráfico, captura y posterior análisis de los protocolos involucrados.

La entrega y aprobación de este Trabajo Práctico es condición necesaria para regularizar o promocionar la asignatura. Esta actividad es de resolución personal.

Actividades

Preparatoria

1) Antes de la realización de este trabajo usted debe preparar sus propios datos para la prueba. Para ello, descargue la plantilla HTML desde la siguiente URL: <http://www.tyr.unlu.edu.ar/pub/TP-Final-template.html> y proceda a completarla con sus datos. Renombre el archivo como **<su-legajo>.html**

Como habrá podido apreciar, la plantilla tiene la referencia a dos imágenes. El nombre las mismas debe respetar el siguiente formato: **<su-legajo>-[1|2].[gif|jpg|png]**.

Ejemplo, **92888.html**, **92888-1.jpg** y **92888-2.jpg**.

Como verá más adelante (en el punto 2), las imágenes estarán alojadas en el servidor con el mnemónico img.orgx.com y serán solo accesibles a través del protocolo HTTPS (por ejemplo: <https://img.orgx.com/92888-1.png>)

Con los tres archivos arme un paquete comprimido y envíelo a florge@unlu.edu.ar con el siguiente "Subject" [TYR-DATOS-TP-FINAL]<legajo>.

Recuerde que es estrictamente necesario contar con estos datos ANTES del día de la realización de este TP (revise el cronograma).



En laboratorio

2) Implemente en el laboratorio las redes de acuerdo al plano de topología adjunto. Configure las interfaces, ruteadores y servicios necesarios, de acuerdo a las siguientes consideraciones:

- La Organización X se vincula a Internet a través de un proveedor de servicios (ISP). Éste, le asignó un bloque de direcciones IP públicas (210.200.12.64/26), el cual es utilizado para la zona de equipos de servicios digitales de la organización.
- Por cuestiones de seguridad, el servidor proxy HTTP (squid) y los equipos de usuarios se encuentran en una red privada (10.10.10.0/24) y acceden al exterior a través del router C, en el cual se implementa traducción de direcciones (NAT). El servidor proxy utiliza el puerto 3128 mediante en cual todos los usuarios acceden al servicio web.
- El servidor DNS maneja la zona **orgx.com** (Organización X) se encuentra en el segmento de red público de la organización.
- El ISP provee dos servidores Web, uno opera en el puerto 80 y sirve sólo páginas html. El segundo (img), implementa solamente HTTPS (en el puerto 443) y sirve imágenes (gif, jpg, png, etc.)

3) Se le proveerá una captura de tráfico de ruteo dinámico que deberá analizar posteriormente.

4) Luego de finalizar la configuración debe realizar la captura (usando Wireshark) de una transferencia completa de la página y sus imágenes, utilizando el mnemónico del servidor web. La captura debe comenzar con el equipo cliente web apagado (las tablas ARP de los ruteadores y hosts deben estar vacías), y finalizar cuando de forma completa se ha logrado cargar la página. La captura original (incluyendo carga de aplicación) debe ser incluida como un anexo del trabajo. Recuerde configurar el proxy en el navegador del cliente.



En su casa

5) Análisis de protocolos

Para la captura de tráfico de ruteo:

- a) Numere cada frame secuencialmente
- b) Haga un diagrama donde muestre la secuencia de intercambio de mensajes del protocolo de ruteo entre los routers y la información de rutas aprendidas en cada paso.

Para la captura de transferencia de la página:

- a) Numere cada frame secuencialmente para poder referenciarlos en las respuestas. Descarte los mensajes que no pertenecen específicamente a esta transferencia.
- b) Confeccione cuadros con la distribución de mensajes por protocolo por capa.
- c) Identifique las conexiones TCP. Por cada una indique: finalidad, sockets de cliente y servidor. Identifique los segmentos de apertura y muestre los parámetros intercambiados en esta instancia.
- d) Para la conexión TCP utilizada para recuperar el archivo html indique la finalidad de cada PDU intercambiada a nivel de transporte y aplicación.
- e) Localice y muestre las diferencias entre las peticiones HTTP y HTTPS (Opcional: Haga un diagrama del intercambio del protocolos SSL en intente explicar el objetivo de los mensajes).
- f) Analice las PDU TCP de la conexión anterior (punto d) mostrando cómo los números de secuencia (desde el ISN), confirmaciones y tamaños de ventana. Trate de identificar variaciones en las ventanas.
- g) Genere un diagrama que muestre cómo sucedieron los intercambios en el tiempo, incluyendo TODOS los dispositivos involucrados.
- h) Compare los headers HTTP del requerimiento del cliente al proxy con respecto del realizado por el proxy al servidor web. Explique las diferencias.
- i) Calcule el overhead total generado para lograr la transferencia. Indique en un gráfico la incidencia de cada protocolo en el overhead total.

