Universidad de Talca
Facultad de Ingeniería
Departamento de Ciencias de la Computación

Gestion de Redes

Laboratorio 1

Introducción al análisis de paquetes con Wireshark.

Profesor: José Letelier (jletelier@utalca.cl)
Alumno Ayudante: Erik Regla (eregla09@alumnos.utalca.cl)

18 de Diciembre del 2015

1. Instalación y uso de Wireshark

Wireshark es un analizador de paquetes de código abierto, multiplataforma, comunmente usado en analisis, resolución de problemas y desarrollo de software y protocolos de comunicaciones.

1. Dirígase a `https://www.wireshark.org/#download` para descargar e instalar la versión apropiada para su sistema. (Se recomienda utilizar *Kali Linux* como distribuición dado que trae esta y otras herramientas comúnmente utilizadas en estudio de redes.)
2. En caso de sistemas Linux, el instalador de su distribución puede preguntar si desea permitir la captura de paquetes sobre los usuarios sin privilegios. Si bien permitir esta opción no afecta el funcionamiento, se recomienda marcar *no*, a momentos pueden ocurrir problemas debido a los permisos que requieren librerías como *libpcap*.

2. Análisis de paquetes ICMP sobre una red local (1.5 pto.)

2.1. Pre-requisitos

1. Inicie una captura sobre la interfaz actualmente conectada.
2. Abra un intérprete de comandos y ejecute `ping 192.168.0.101`, para realizar *ping* a una máquina dentro de la red local.
3. Espere 5 segundos.
4. Detenga la captura de datos.

[1] puede utilizar el filtro `icmp` para ocultar todos los paquetes que no correspondan a este protocolo.

2.2. Actividad

Analice los paquetes capturados y responda las siguientes preguntas: [1]

1. Identifique un paquete ICMP enviado desde su equipo.
   a) ¿Cuál es la dirección física de origen?
   b) ¿Cuál es la dirección física de destino?
   c) ¿Coinciden estas direcciones con las expuestas por las máquinas?
2. Identifique un paquete ICMP recibido como respuesta al paquete anterior.
   a) ¿Cuál es la dirección física de origen?
   b) ¿Cuál es la dirección física de destino?
   c) ¿Coinciden estas direcciones con las expuestas por las máquinas?
3. El protocolo Ethernet II utiliza campos de *fuente (source)*, *destino (destination)*, *versión (version)*. Identifíquelas.
4. El protocolo ICMP (Internet Control Message Protocol), como el *tipo (type)*, *suma de verificación (checksum)*,*número de secuencia (sequence number)*, *timestamps* . Identifíquelas.
5. ¿Por qué la información del protocolo ICMP está al final del paquete?
6. Repita el ejercicio pero esta vez realizando `ping 192.168.0.150`. ¿Nota alguna diferencia entre los paquetes capturados cuando el host existe? [2]

3. Análisis de paquetes ICMP sobre una red extendida (1.5 pto.)

3.1. Pre-requisitos

1. Inicie una captura sobre la interfaz actualmente conectada.
2. Abra un intérprete de comandos y ejecute `ping www.utalca.cl`, para realizar *ping* a una máquina dentro de la red local.
3. Espere 5 segundos.
4. Detenga la captura de datos.

3.2. Actividad

Analice los paquetes capturados y responda las siguientes preguntas: [3]

[2] Es posible que sea necesario remover los filtros para volver este cambio notable en Wireshark.
[3] puede utilizar el filtro `icmp` para ocultar todos los paquetes que no correspondan a este protocolo.

1. Identifique un paquete ICMP enviado desde su equipo.
   a) ¿Cuál es la dirección física de origen?
   b) ¿Cuál es la dirección física de destino?
   c) ¿Coinciden estas direcciones con las expuestas por las máquinas?
2. Identifique un paquete ICMP recibido como respuesta al paquete anterior.
   a) ¿Cuál es la dirección física de origen?
   b) ¿Cuál es la dirección física de destino?
   c) ¿Coinciden estas direcciones con las expuestas por las máquinas?
3. El protocolo Ethernet II posee campos de *fuente (source)*, *destino (destination)*, *versión (version)*. Identifíquelas.
4. El protocolo ICMP (Internet Control Message Protocol), como el *tipo (type)*, *suma de verificación (checksum)*,*número de secuencia (sequence number)*, *timestamps* . Identifíquelas.

4. Análisis de paquetes TCP (1.5 pto.)

4.1. Pre-requisitos

1. Inicie una captura sobre la interfaz actualmente conectada.
2. Con un navegador web abra el sitio `www.utalca.cl`, para realizar *ping* a una máquina dentro de la red local.
3. Espere 5 segundos.
4. Detenga la captura de datos.

4.2. Actividad

Analice los paquetes capturados y responda las siguientes preguntas: [4]

1. Identifique una petición GET enviada desde su equipo en la cual se recupere un archivo JavaScript.
   a) Indique los campos que exponen los paquetes del protocolo HTTP.
   b) Indique las direcciones físicas de origen y destino y contrástelas con las presentes en su maquina. ¿La dirección física de destino a que máquina pertenece? Justifique.
   c) Identifique el host al cual la petición fue realizada.

[4] puede utilizar el filtro `http` para visualizar solo paquetes que correspondan al protocolo HTTP/1.1.

2. Identifique un paquete en el cual se recupere una imagen JPEG y otro en el cual se recupere un archivo PNG desde el servidor.

   a) Indique las diferencias entre el paquete recuperado para la imágen JPEG y PNG.

   b) Como podrá haber observado, Wireshark muestra un apartado dentro del examinador de paquetes que dice `Reassembled TCP Segments`. ¿Qué significa esto?

5. Análisis de trama IPv6 (1.5 pto.)

5.1. Pre-requisitos

1. Inicie una captura sobre la interfaz actualmente conectada.
2. Abra un intérprete de comandos y ejecute `ping6 2001::100`, para realizar *ping6* a una máquina dentro de la red local.
3. Espere 5 segundos.
4. Detenga la captura de datos.

5.2. Actividad

Analice los paquetes capturados y responda las siguientes preguntas: [5]

1. Identifique un paquete ICMPv6 enviado desde su equipo.

   a) ¿Cuál es la dirección física de origen?

   b) ¿Cuál es la dirección física de destino?

2. Identifique un paquete ICMPv6 recibido en su equipo.

   a) ¿Cuál es la dirección física de origen?

   b) ¿Cuál es la dirección física de destino?

3. Indique algunas diferencias notables entre las tramas ICMP y ICMPv6.
4. Repita el ejercicio pero esta vez realizando `ping6 2001::150`. ¿Nota alguna diferencia en los paquetes enviados y recibidos por medio de este protocolo en comparación a ICMPv4?

6. Reflexión

Como podrá haber notado, Wireshark solo captura los paquetes que están siendo transmitidos en la interfaz destino. En base a los ejercicios anteriores, de querer capturar paquetes enviados por otros equipos dentro de la red local, ¿Qué tendría que hacer para poder capturarlos?

[5] puede utilizar el filtro `icmpv6` para visualizar solo paquetes que correspondan al protocolo ICMPv6