UNIVERSIDAD SIMÓN BOLÍVAR

Departamento de Computación y Tecnología de la Información

TRIMESTRE SEPTIEMBRE-DICIEMBRE 2016

REDES DE COMPUTADORES I (CI 4835)

ASIGNACIÓN N°2

Objetivo General: Familiarizarse con el uso de analizadores de tráfico para capturar y analizar las tramas 802.11 que viajan por las redes locales inalámbricas WLAN (más conocidas como Wi-Fi)

Objetivos Específicos: Al finalizar esta actividad el estudiante deberá estar en capacidad de:

- ✓ Analizar redes inalámbricas por medio de un analizador de tráfico
- ✓ Detectar problemas causados por fallas, congestión o brechas de seguridad
- ✓ Entender cómo funcionan los protocolos de comunicación en redes inalámbricas

PLANTEAMIENTO DEL PROBLEMA

Existe una gran variedad de herramientas que permiten capturar los datos que viajan por las redes de comunicación y posteriormente analizarlos. Se les conoce como: analizadores de protocolos, analizadores de redes, analizadores de tráfico, o sniffers (jerga técnica proveniente del inglés). Ellos son muy útiles para los ingenieros, técnicos y administradores de redes, ya que por medio de la monitorización se permite encontrar y solucionar variados y complejos problemas del tráfico; además, son una excelente ayuda didáctica para entender cómo funcionan los protocolos de las redes modernas. Sin embargo, representan un arma peligrosa en mano de personas mal intencionadas porque pueden capturar datos confidenciales (ej. contraseñas) que no estén encriptadas.

Hoy día existen muchos productos disponibles, la mayoría comerciales, pero también los hay gratuitos y de código abierto. Entre estos últimos se encuentra el famoso Wireshark® que es quizás el más popular. Otros productos conocidos son: Microsoft Network Monitor®, OmniPeek®, CommView® y CommView for WiFi.

La mayoría de los analizadores de red son productos de software que utilizan la interfaz de la red (NIC, esto es Network Interface Card) para capturar indiscriminadamente

todo el tráfico de la red que esté a su alcance en vez de acceder solamente al tráfico enviado específicamente a esa máquina.

Normalmente una interfaz Ethernet, por las normas operativas, descartaría cualquier tráfico que no vaya dirigido a ella o a la dirección de difusión de la red, por lo que el analizador deberá hacer que la interfaz entre en un estado especial denominado ***modo promiscuo***. Eso, al igual que un protocolo que físicamente permita compartir un mismo medio de transmisión entre distintos nodos de la red, permitiría acceder a paquetes ajenos. En las redes inalámbricas la captura clandestina del tráfico es relativamente más fácil que en las redes cableadas, donde un intruso que busque acceso a una LAN cableada se enfrenta irremediablemente con el problema de la conexión a la misma y es imprescindible una conexión física al cable de la red por donde circulan los datos o a los dispositivos físicos de comunicación que la conforman. En una WLAN el problema del intruso se torna etéreo: las señales de radio a través de las cuales se transmite la información y que utilizan los dispositivos de red que la conforman, se propagan con significativa libertad a través del espacio, estando por lo tanto al alcance de cualquiera que tenga capacidad para interceptarlas. Al intruso le basta permanecer en el área de cobertura que puede ser muy extensa, para estar en contacto con la red local; puede incluso estar en movimiento.

Las tarjetas inalámbricas, como caso especial, no pueden trabajar en modo promiscuo sino en ***modo monitor***, lo cual esencialmente significan que pueden capturar el tráfico inalámbrico a su alrededor, pero no pueden transmitir.

Ustedes como miembros de Redes de Computadores I, tienen la misión de capturar y analizar el tráfico que viaje por una red inalámbrica (WIFI), deberán escoger el escenario a trabajar durante 7 días; para ello deberá levantar un informe que contenga los siguientes aspectos:

- ✓ Describa los dispositivos de Hardware que conforma la red. Justifique
- ✓ ¿Cuál fue el o los softwares utilizados y por qué? Justifique
- ✓ Explique el funcionamiento de la Red
- ✓ Vea y analice la red, así como el tráfico (gestión, control y datos) que viaja a través del tiempo
- ✓ Conserve y almacene datos de la red para manejar reportes y tendencias
- ✓ Genere reportes (estadísticas) sustentados para justificar las necesidades de actualización de la red
- ✓ Además, el sistema deberá disparar de manera automática una alerta de cuando la red falla a fin de tomar decisiones a tiempo y reforzar el sistema de seguridad

CONDICIONES DE ENTREGA

- Realice la captura de pantalla detallada de cada procedimiento, a modo de poder observar los pasos que realizó.
- Deberá enviarse al correo del docente encargado y subirlo en el Aula Virtual hasta las 11:50 p.m
- Se aceptará la entrega hasta el jueves de semana 11 (24 de noviembre de 2016)
- El acceso para subir los archivos será cerrado luego de la hora establecida, por lo tanto se recomienda no esperar hasta la última hora
- Cualquier demora podrá dar la potestad al docente de no aceptar el trabajo
- Sea organizado en el documento que será entregado, incluya portada, contenido, descripción del problema a resolver, conclusiones y recomendaciones entre otros; se evaluará la presentación.
- Los equipos deben ser de dos (2) estudiantes. En caso de ser necesario sus integrantes deberán asegurarse de poder explicar, a cabalidad, la distribución del trabajo.
- Cada miembro del equipo debe estar en capacidad de comprender y desarrollar cualquier parte del trabajo, incluso aunque no le haya sido asignada originalmente ya que podrá ser interrogado al respecto durante la corrección del mismo
- Aquellas personas que no muestren un dominio de los detalles del proyecto no tendrán puntos en la evaluación
- Ambos deben estar inscritos en el curso y en aula virtual. Si estas condiciones no se cumplen, el evaluador del proyecto podrá reprobar al integrante que no cumpla con las mismas.
- Cualquier caso de plagio será severamente castigado, no será evaluado ninguno de los proyectos involucrados y serán aplicadas las sanciones correspondientes establecidas en los reglamentos de la universidad
- La entrega será con un archivo y se identificará de la siguiente manera:

Apellido1_Apellido2_X.pdf

X será reemplazado por el término Monitoreo y Apellido1 y Apellido2 corresponden a los apellidos de los integrantes del grupo (por ejemplo, Alvarez_Torrealba_Monitoreo.pdf)

ÉXITO!

Noviembre 2016/GDRCI