Único Curso del Año 2018

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Domingos 17 y 24 de Junio del 2018

De 9:00 am a 12:15 pm (UTC -05:00) – 6 horas en Total

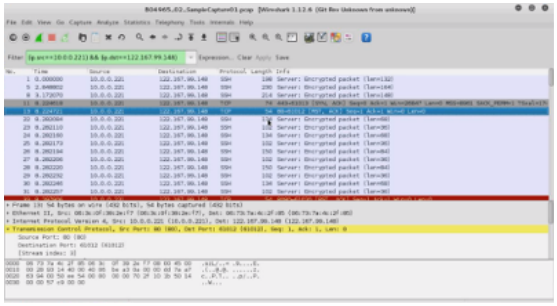
1. Presentación:

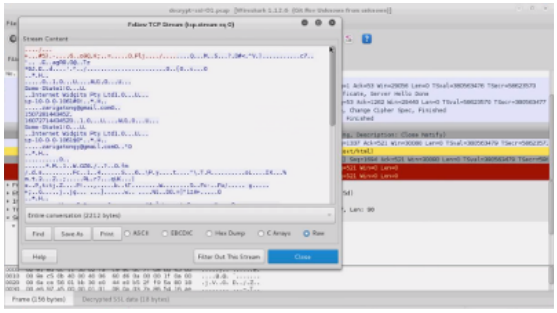
Wireshark es un analizador para protocolos de red. El cual permite capturar e interactivamente navegar el tráfico fluyendo sobre una red de computadoras. Incluye un conjunto de funcionalidades valiosas y poderosas, además de ser la herramienta más popular a nivel mundial de este tipo. Se ejecuta en la mayoría de plataformas de cómputo, incluyendo Windows, OSX, Linux, y UNIX. Es utilizado alrededor del mundo por profesionales en redes, expertos en seguridad, desarrolladores y educadores. Esta disponible libremente como programa “open source”, y está liberado bajo la licencia GNU versión 2. Wireshark es desarrollado y activamente mantenido por un equipo global de expertos en protocolos.

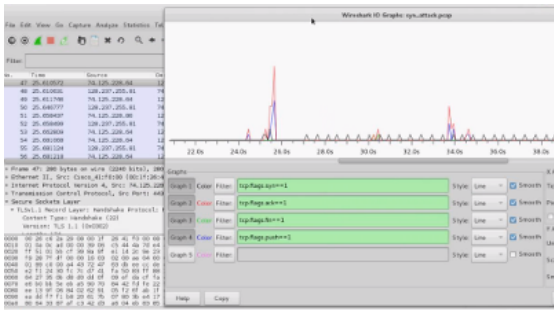
El curso práctico de Wireshark enseña a los participantes a identificar, conocer y resolver temas relacionados a los protocolos, las redes y la seguridad, además de ver como Wireshark ayuda a analizar patrones permitiendo a sus funcionalidades solucionarlas efectivamente. Este curso utiliza archivos con capturas de paquetes previamente realizados, como también paquetes capturados en tiempo real. Estos son utilizados durante la explicación y desarrollo de los ejercicios.

2. Temario:

- Analizadores de Paquetes
- Usos de Analizadores de Paquetes
- Introducción a Wireshark
- Usos y Características de Wireshark
- Dumpcap y Tshark
- Capturar Paquetes
- Guía para Capturar Paquetes
- Opciones de Filtros para Captura
- Interfaz de Usuario de Wireshark
- Barra de herramientas de Filtros
- Técnicas par Filtrar
- Paneles de Listado de Paquetes, Detalles de Paquetes y Bytes de Paquetes
- Funcionalidades de Wireshark
- Decodificación
- Gráficos de Entrada y Salida
- Seguir el Flujo de Datos
- Exportar Paquetes de Datos
- Analizar una Red TCP
- Revisión del protocolo TCP
- Establecimiento y Limpieza de Conexión TCP
- Comunicación de Datos
- Secuencia de Cierre TCP
- Análisis de la Secuencia TCP
- Analizar SSL/TLS
- Introducción a SSL/TLS
- Saludo SSL/TLS
- Intercambio de Llaves
- Descifrando SSL/TLS
- Analizar Protocolos de la Capa de Aplicación
- Protocolos DHCP, DNS, HTTP
- Filtros de Wireshark para Protocolos
- Capturar WLAN
- Configuración para la Captura WLAN
- Analizar Redes Wi-Fi
- Análisis de Seguridad
- Ataques DOS (Negación de Servicio)
- Escaneos







3. Material:

Se sugiere al participante tener instalado la versión más reciente de Wireshark, ya sea en Windows o GNU/Linux. Wireshark puede ser descargado desde los siguientes enlaces.

Wireshark: https://www.wireshark.org/#download

Enlace de Descarga (Windows 32-Bit): https://1.na.dl.wireshark.org/win32/Wireshark-win32-2.6.1.exe
Enlace de Descarga (Windows 64-Bit): https://1.na.dl.wireshark.org/win64/Wireshark-win64-2.6.1.exe

Enlace de descarga (Linux): Se sugiere utilizar Kali Linux, o utilizar el gestor de paquetes de su distribución Linux para instalar Wireshark.

También se sugiere descargar algunos de los siguientes archivos para realizar las demostraciones.

Capturas de Ejemplo: https://wiki.wireshark.org/SampleCaptures

[*] Si el participante lo requiere se le puede enviar un DVD con todo el material utilizado añadiendo S/. 55 Soles por el concepto de gastos de envío hacia cualquier lugar del Perú.

4. Día y Horario:

La duración total del curso es de 6 (seis) horas. El Curso se dictará en los siguientes días y horarios.

Domingos 17 y 24 de Junio del 2018
De 9:00 am a 12:15 pm (UTC -05:00) - 6 Horas en Total

[*] No habrá reprogramaciones. El Curso se dictará **sin** ningún requisito mínimo de participantes.

5. Inversión y Forma de Pago:

El Curso tiene un costo de:

S/. 165 Soles o $ 50 Dólares

El pago del Curso se realiza mediante un depósito bancario en la siguiente cuenta:

ScotiaBank
Cuenta de Ahorros en Soles: 324-0003164
A nombre de: Alonso Eduardo Caballero Quezada

Una vez realizado el depósito, enviar por favor el comprobante escaneado a la siguiente dirección de correo electrónico: **caballero.alonso@gmail.com**.

Otros Países

Para residentes en otros países el pago se realiza mediante una transferencia de dinero utilizando Western Union. Por favor escribir un mensaje de correo electrónico a **caballero.alonso@gmail.com**. para coordinarlos datos para realizar la transferencia.

Confirmado el depósito o transferencia, se enviará al correo electrónico del participante, los datos necesarios para conectarse hacia el sistema y poder participar en el curso.

6. Más Información:

Si desea mayor información sobre el Curso de Wireshark, tiene a su disposición los siguientes mecanismos de contacto:

Correo electrónico: caballero.alonso@gmail.com

Vía Web: http://www.reydes.com

Celular: +51 949304030

7. Instructor:

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals y y Phishing Countermeasures. Ha sido instructor en el OWASP LATAM Tour Lima, Perú del año 2014 y expositor en el 0x11 OWASP Perú Chapter Meeting 2016, además de Conferencista en PERUHACK 2014, instructor en PERUHACK2016NOT, y conferencista en 8.8 Lucky Perú 2017. Cuenta con más de catorce años de experiencia en el área y desde hace diez años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Perteneció por muchos años al grupo internacional de seguridad RareGaZz y al grupo peruano de seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal es: http://www.ReYDeS.com.