Contenido del Curso

Experto en WIRESHARK

La guía completa para principiantes

YACHA

Sección 1: Bienvenida

***Objetivo de la sección**: Conocer al curso e instructor*

- Comienza aquí ·
- Contenido del curso *¡Estás aquí!
- **Recurso**: Enlaces útiles

Sección 2: Explora a Wireshark

***Objetivo de la sección**: Entender cómo funciona Wireshark*

- Introducción "Explora a Wireshark"
- **Recurso**: Modelo TCP/IP
- ¿Qué es Wireshark?
- **Comparte**: Metas personales
- ¿Cómo funciona Wireshark?
- Conceptos de TCP/IP, Parte 1
- Conceptos de TCP/IP, Parte 2
- Descargar e instalar Wireshark
- Wiki y foro oficiales
- Explorar interfaz gráfica & primera captura de tráfico
- **Laboratorio 1**: TCP/IP en Wireshark
- Tráfico de red típico
- Tráfico de fondo
- **Laboratorio 2**: Detecta tu propio tráfico de fondo
- **Comparte**: ¿Hay algo no usual en tu tráfico de fondo?
- Archivos de captura de tráfico
- **Laboratorio 3**: Abrir un archivo de captura no-nativo
- **Reto 1**
- **Recurso**: Solución del Reto 1
- Resumen "Explora a Wireshark"

Sección 3: Personalizar Wireshark

***Objetivo de la sección**: Cómo personalizar Wireshark de acuerdo al tráfico analizado*

- Introducción "Personalizar Wireshark"
- Columnas
- **Laboratorio 4**: Resaltar URLs de tu tráfico
- Disectores
- Puertos no-estándar
- Ajustes de presentación
- **Laboratorio 5**: Ajustes clave de presentación
- Perfiles
- **Laboratorio 6**: Crear un perfil
- Archivos de configuración

- **Laboratorio 7**: Importar un perfil
- **Comparte**: ¿qué perfil crearías para tus necesidades?
- Detección de latencia
- **Laboratorio 8**: Detectar la latencia y su origen
- **Reto 2**
- **Recurso**: Solución del Reto 2
- Resumen "Personalizar Wireshark"

Sección 4: Capturar tráfico de red

***Objetivo de la sección**: Cómo capturar el tráfico que necesitas*

- Introducción "Capturar tráfico de red"
- **Recurso**: Listado de filtros de captura
- Demasiados paquetes
- Técnicas de captura
- **Laboratorio 9**: Captura en anillo
- Reducir el tráfico capturado
- Capturar tráfico de nodos específicos
- **Laboratorio 10**: Capturar el tráfico de todos los demás
- Capturar tráfico de una aplicación
- **Comparte**: Tráfico de fondo + filtros de captura
- **Laboratorio 11**: Filtros de captura
- **Reto 3**
- **Recurso**: Solución del Reto 3
- Resumen "Capturar tráfico de red"

Sección 5: Visualizar tráfico de interés

***Objetivo de la sección**: Cómo presentar el tráfico objetivo*

- Introducción "Visualizar tráfico de interés"
- **Recurso**: Lista de filtros de visualización
- Filtros de visualización
- Filtrado en la capa de aplicación
- Filtrar tráfico de nodos específicos
- Expandir filtros de visualización
- Aplicar filtros de manera rápida
- **Laboratorio 12**: Filtrar nodo + aplicación
- **Comparte**: ¿qué combinación de filtros utilizarías más?
- Filtrar una conversación TCP/UDP
- **Laboratorio 13**: Filtrar una conversación TCP
- Revisión de filtro aplicado
- Filtrar una palabra
- **Laboratorio 14**: Encontrar la palabra escondida
- **Reto 4**

- **Recurso**: Solución del Reto 4
- Resumen "Visualizar tráfico de interés"

Sección 6: Analizar tráfico de interés

***Objetivo de la sección**: Cómo analizar capturas desde diferentes ángulos*

- Introducción "Analizar tráfico de interés"
- **Recurso**: Bases de datos GeoIP
- Reglas de coloreado
- Crear reglas de coloreado
- Scrollbar inteligente
- Exportar paquetes de interés
- ¿Quién está hablando con quién?
- Identificar a top-talkers
- **Laboratorio 15**: Identificar a los top-talkers de tu red
- GeoIP
- **Laboratorio 16**: Identifica las ubicaciones de tu tráfico
- **Comparte**: ¿cuál es el país más inesperado de tu captura?
- Listar aplicaciones de red
- Graficar el ancho de banda
- **Laboratorio 17**: Graficar el ancho de banda de tu red
- Añadir comentarios
- **Reto 5**
- **Recurso**: Solución del Reto 5
- Resumen "Analizar tráfico de interés"

Sección 7: Reensamblar archivos

***Objetivo de la sección**: Cómo extraer los datos capturados*

- Introducción "Reensamblar archivos"
- Reensamblado de HTTP
- Reensamblado de Telnet
- Reensamblado de DNS
- **Laboratorio 18**: Seguir una conversación y analizar su flujo
- Extraer una imagen de una captura FTP
- Extraer una imagen de una captura HTTP
- **Laboratorio 19**: Extraer imágenes de una captura
- Reproducir una conversación VoIP
- **Laboratorio 20**: Escuchar la llamada capturada
- **Comparte**: ¿qué otros archivos o datos podrías capturar?
- **Reto 6**
- **Recurso**: Solución del Reto 6
- Resumen "Reensamblar archivos"

Sección 8: Despedida

***Objetivo de la sección**: Siguientes pasos*

- ¡Lo lograste!
- **Recurso**: Sigue practicando

La vida no se trata de

HACER PLANES

Se trata de

RESULTADOS

2020 Yacha