Basque CyberSecurity Centre

Tshark cheat sheet

Analizador de tráfico de red, por línea de comandos, que permite capturar datos de paquetes de una red, o leer paquetes de un archivo guardado previamente.

(El formato de la cheat sheet es descripción de la instrucción, instrucción en negrita)

1. Opciones de interfaz de captura

- Nombre o índice de la interfaz (el valor predeterminado es 1º non-loopback)
  -i < interfaz >
- Filtro de paquetes en la sintaxis del filtro Libpcap
  -f < filtro de captura>
- Deshabilitar la captura en modo promiscuo
  -p
- Tamaño del búfer del kernel (def. 2MB)
  -B < tamaño del búfer >
- Tipo de capa de enlace (por defecto al primero apropiado)
  -y < tipo de vínculo >
- Imprimir lista de interfaces y salir
  -D
- Imprimir lista de tipos de capa de vínculo y salir
  -L

2. Condiciones de detención y salida de captura

- Parar después de n paquetes (por defecto a infinito)
  -c < recuento de paquetes >
  -a < condición de autostop >
- Salida de captura
  -b <ringbuffer opt>

3. Opciones de procesamiento

- Realizar un análisis de dos pasadas
  -2
- Filtro de lectura de paquetes en la sintaxis del filtro de visualización wireshark
  -R < filtro de lectura >
- Filtro de lectura de paquetes en la sintaxis del filtro de visualización wireshark
  -Y < filtro de visualización >
- Deshabilitar todas las resoluciones de nombres
  -n
- Habilitar resoluciones de nombres específicos:
  -N < indicadores de resolución de nombre >
- Decodificar como. Consultar la página de man Tshark para obtener más información
  -d < tipo de capa >==<selector>,<decode_as_protocol>
- Leer una lista de entradas de un archivo hosts que luego se escribirá en un archivo de captura (implica -W n)
  -H <hosts file>
- Deshabilitar la disección de<proto_name>
  --disable-protocol <proto_name>
- Habilitar la disección del protocolo heurístico
  --enable-heuristic <short_name>
- Deshabilitar la disección del protocolo heurístico
  --disable-heuristic <short_name>

4. Varias opciones

- Mostrar ayuda y salir
  -h
- Mostrar información de la versión y salir
  -v
- Anular la configuración de preferencias
  -o <nombre>:<valor>
- Archivo keytab que se utilizará para el descifrado Kerberos
  -K <keytab>
- Volcar uno de los varios informes disponibles y salir
  -G < Informe >
  informe predeterminado ="fields"
  usar -G ? para obtener más ayuda

Basque CyberSecurity Centre

5. Opciones del archivo de salida

- Escribir paquetes en un archivo de formato PCAP denominado Outfile

  -w <outfile|->

- Comenzar con el perfil de configuración especificado

  -C < perfil de configuración>

- Establecer el tipo de archivo de salida (por defecto es PCAP-NG), -F sin ninguna especificación, mostrará los tipos de archivo

  -F < tipo de archivo de salida >

- Agregar salida del árbol de paquetes (detalles del paquete)

  -V

- Mostrar sólo los detalles del paquete de protocolos (separados por comas)

  -O < protocolos >

- Imprimir resumen de paquetes incluso mientras se escribe en un archivo

  -P

- El separador de líneas para imprimir entre paquetes

  -S < separador >

- Agregar salida de volcado hexadecimal y ASCII (bytes de paquetes)

  -x

- Formato de salida de texto (por defecto texto)

  -T pdml|ps|psml|text|fields

- Campo para imprimir si -Tfields seleccionado (tcp.port, ws.col.info). Esta opción se puede repetir para imprimir varios campos.

  -e <field>

- Establece opciones para la salida cuando se selecciona -Tfields :

  -E < opción campos >=< valor >

header= y|n	activar y desactivar los encabezados
separator=/t|/s|<char>	seleccionar tabulación, espacio, carácter imprimible como separador
occurence=f|L|a	imprimir primero, último o todas las ocurrencias de cada campo
aggregator=,|/s|/<char>	seleccionar coma, espacio, caracter imprimible como agregador
quote=d|s|n	seleccione comillas dobles, simples o nulos para los valores

- Formato de salida de marcas de tiempo (def: r rel. a first)

  -t a|ad|d|dd|e|r|u|ud

- Formato de salida de segundos (def: s - segundos)

  -u s|hms|

- Vaciar la salida estándar después de cada paquete

  -l

- Sólo registra los errores verdaderos en stder

  -Q

- Habilitar el acceso de lectura de grupo en los archivos de salida

  -g

- Guarda información adicional en el archivo, si es compatible

  -W n

- Escribir información de resolución de direcciones de red

  n= Opciones de extension

  Consultar para obtener más información sobre opciones https://www.wireshark.org/docs/man-pages/tshark.html

  -X <key>:<valor>

- Varias estadísticas

  -z <statistics>

- Agregar un comentario de captura al archivo de salida recién creado (sólo para el formato PCAPNG)

  --capture-comment <comentario>