

Lab 35: IDENTIFICAR UN CLIENTE SOBRECARGADO

Paso 1: Abra http-download101.pcapng

Paso 2: haga clic en el botón experto información en la barra de estado paso

3: expanda las secciones de advertencia y nota para examinar los problemas detectados en este archivo de seguimiento

Paso 4: En la sección de advertencias, haga clic en 363: La ventana TCP especificada por el receptor ahora está completamente llena. wireshark salta al paquete 363 en el archivo de seguimiento. Aquí es donde wireshark indica que el cliente va a ejecutar el espacio del búfer de recepción Si mira más allá del problema de la ventana cero en este archivo de seguimiento, puede ver que el cliente se recupera con los paquetes de actualización de la ventana en los marcos 377 y 378. por qué esta es una condición a tener en cuenta en su red

The screenshot displays the Wireshark network protocol analyzer interface. The top pane shows the packet list with columns: No., Time, Source, Destination, Protocol, and Length. Packet 363 is selected, showing a TCP reset (RST) from 61.8.0.17 to 10.0.52.164. The bottom pane shows the expert view with columns: Paquete, Resumen, Grupo, Protocolo, and Recuento. A warning is displayed for packet 363: 'Warning: TCP window specified by the receiver is now completely full'. The expert view also shows other warnings and notes related to the TCP connection, such as 'Warning: This frame is a (suspected) out-of-order segment' and 'Note: TCP keep-alive segment'.

No.	Time	Source	Destination	Protocol	Length
356	3.619988	61.8.0.17	10.0.52.164	TCP	1514
357	3.626325	61.8.0.17	10.0.52.164	TCP	1514
358	3.626343	10.0.52.164	61.8.0.17	TCP	54
359	3.636969	61.8.0.17	10.0.52.164	TCP	1514
360	3.643310	61.8.0.17	10.0.52.164	TCP	1514
361	3.643329	10.0.52.164	61.8.0.17	TCP	54
362	3.668828	61.8.0.17	10.0.52.164	TCP	1514
363	3.675039	61.8.0.17	10.0.52.164	TCP	1514
364	3.675080	10.0.52.164	61.8.0.17	TCP	54
365	4.342163	61.8.0.17	10.0.52.164	TCP	60

Paquete	Resumen	Grupo	Protocolo	Recuento
> Warning	Connection reset (RST)	Sequence	TCP	1
> Warning	TCP Zero Window segment	Sequence	TCP	7
> Warning	TCP window specified by the receiver is now completely full	Sequence	TCP	1
> Warning	[TCP Window Full] 80 → 2550 [ACK] Seq=296710 Ack=446 ...	Sequence	TCP	1
> Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	83
> Warning	D-SACK Sequence	Sequence	TCP	970
> Warning	Previous segment(s) not captured (common at capture sta...	Sequence	TCP	100
> Note	TCP keep-alive segment	Sequence	TCP	6
> Note	This frame is a (suspected) fast retransmission	Sequence	TCP	40
> Note	This frame is a (suspected) retransmission	Sequence	TCP	70
> Note	Duplicate ACK (#1)	Sequence	TCP	846
> Chat	TCP window update	Sequence	TCP	163
> Chat	GET/openoffice/stable/2.0.0/OOo_2.0.0_Win32Intel_install...	Sequence	HTTP	1
> Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	1
> Chat	Connection establish request (SYN): server port 80	Sequence	TCP	1

Paso 5: cuando haya terminado de revisar la información del experto, haga clic en el botón cerrar en la ventana de información del experto