

Análisis de conexiones TCP con Wireshark (negociación en tres pasos y cierre de una conexión)

Pasos necesarios para analizar las conexiones TCP con Wireshark:

- Enviar un mensaje entre un cliente y un servidor
 - Capturar, analizar y filtrar el tráfico capturado detectando la negociación en tres pasos y el cierre de la conexión
-

Enviar un mensaje entre un cliente y un servidor

Cliente envía un mensaje al servidor:

Enviar un mensaje mediante PowerShell

[crayon-6a9d619c37462939760225/]

Servidor que recibe el mensaje que envía el cliente:

Recibir el mensaje mediante PowerShell

[crayon-6a9d619c37468718022511/]

Capturar, analizar y filtrar el tráfico capturado detectando la negociación en tres pasos y el

cierre de la conexión



Wireshark · Expert Information · wireshark_pcapng_E16D7C2B-7668-45AC-90BA-DFB681FB100E_201603...

Severity	Group	Protocol	Count
Chat	Sequence	TCP	4
3: Connection establish request (SYN): server port 5556			
4: Connection establish acknowledge (SYN+ACK): server port 5556			
7: Connection finish (FIN)			
9: Connection finish (FIN)			
Chat	Sequence	HTTP	1

Display filter: "tcp.stream eq 0"

☐ Limit to Display Filter

Search:

Show...

Close

Help