ALUMNO: Adolfo Tun Dzul **MATRÍCULA:** 170300124 **TURNO:** Vespertino

MATERIA: Interconectividad de redes

#tarea997

En PDF, investigar sobre Flags de TCP y sus combinaciones

FLAGS DE TCP Y SUS COMBINACIONES

Las banderas TCP se utilizan dentro de las transferencias de paquetes TCP para indicar un estado de conexión particular o proporcionar información adicional. Por lo tanto, se pueden usar para solucionar problemas o para controlar cómo se maneja una conexión en particular. Hay algunas banderas TCP que se usan mucho más comúnmente que otros como "SYN", "ACK" y "FIN".

- **SYN:** el SYN, o Flag de sincronización, se utiliza como primer paso para establecer un protocolo de enlace de tres vías entre dos hosts. Solo el primer paquete del remitente y el receptor debe tener este indicador establecido.

- **ACK:** Flag ACK, que significa "Acuse de recibo", se usa para acusar recibo exitoso de un paquete. El receptor envía un ACK y un SYN en el segundo paso del proceso de enlace de 3 vías para decirle al remitente que recibió su paquete inicial.

- **FIN:** Flag FIN, que significa "Finalizado", significa que no hay más datos del remitente. Por lo tanto, se usa en el último paquete enviado por el remitente.

- **URG:** Flag URG se utiliza para notificar al receptor que procese los paquetes urgentes antes de procesar todos los demás paquetes. El receptor será notificado cuando se hayan recibido todos los datos urgentes conocidos.

- **PSH:** Flag PSH, que significa "Push", es algo similar al indicador URG y le dice al receptor que procese estos paquetes a medida que se reciben en lugar de almacenarlos en el búfer.

- **RST:** Flag RST, que significa "Restablecer", se envía desde el receptor al remitente cuando se envía un paquete a un host particular que no lo esperaba.

- **ECE:** este indicador es responsable de indicar si el par TCP es compatible con ECN.

- **CWR:** el host emisor utiliza la bandera CWR, que significa Congestion Window Reduced, para indicar que recibió un paquete con el conjunto de indicadores ECE.

- **NS (experimental):** Flag NS, que significa Nonce Sum, sigue siendo un indicador experimental utilizado para ayudar a proteger contra el ocultamiento malicioso accidental de paquetes del remitente.

COMBINACIÓN DE BANDERA TCP NORMAL

1.- ***SYN, SYN ACK y ACK*** se utilizan durante el protocolo de enlace de tres vías que establece una conexión TCP.

2. - Excepto por el paquete ***SYN*** inicial, cada paquete en una conexión debe tener el bit ACK establecido.

3. - ***FIN ACK y ACK*** se utilizan durante el desarmado elegante de una conexión existente.

4. - ***RST ACK*** se puede usar para terminar inmediatamente una conexión existente.

5. - Los paquetes durante la parte de "conversación" de la conexión (después del apretón de manos de tres vías, pero antes del desmantelamiento o finalización) contienen solo un ***ACK*** por defecto.

6. -Opcionalmente, también pueden contener ***PSH y / o URG.***

COMBINACIÓN DE BANDERA TCP ANORMAL

1. - ***SYN FIN*** es probablemente la combinación ilegal más conocida. Recuerde que SYN se usa para iniciar una conexión, mientras que FIN se usa para finalizar una conexión existente. No tiene sentido realizar ambas acciones al mismo tiempo. Muchas herramientas de escaneo usan paquetes SYN FIN, porque muchos sistemas de detección de intrusos no los detectaron en el pasado, aunque la mayoría lo hace ahora. Puede asumir con seguridad que cualquier paquete SYN FIN que vea es malicioso.

2. - ***SYN FIN PSH, SYN FIN RST, SYN FIN RST PSH*** y otras variantes en ***SYN FIN*** también existen. Los atacantes pueden utilizar estos paquetes y saben que los sistemas de detección de intrusos pueden estar buscando paquetes con solo el

conjunto de bits SYN y FIN, no conjuntos de bits adicionales. Nuevamente, estos son claramente maliciosos.

3. - Los paquetes nunca deben contener solo una bandera ***FIN***. Los paquetes FIN se usan con frecuencia para escaneos de puertos, mapeo de redes y otras actividades ocultas.

4. - Algunos paquetes no tienen absolutamente ninguna marca establecida; estos se denominan paquetes "nulos". Es ilegal tener un paquete sin banderas establecidas.

Referencias

TCP Flags. (04 de octubre de 2018). Obtenido de Keycdn: https://www.keycdn.com/support/tcp-flags

Whitehats. (24 de enero de 2020). Obtenido de Intrusion Analyst Packet Header Chart: http://www.whitehats.ca/main/members/Seeker/seeker_tcp_header/seeker_tcp_header.html