Tema 9.9.2.6.EnriqueGomezTagle

martes, 27 de febrero de 2024 21:22

Enrique Ulises Báez Gómez Tagle – 0241823 - 0241823@up.edu.mx
UP. 2024. Ene-Jun. Hackeo Ético y Recuperación Ante Desastres – Yoel Ledo Mezquita

¿Cuál es el número de puerto de origen de TCP?

51800

¿Cómo clasificarían el puerto de origen?

Dinamico o Privado

¿Cuál es el número de puerto de destino de TCP?

80

¿Cómo clasificarían el puerto de destino?

Conocido, registrado (HTTP o web)

¿Qué marcadores están establecidos?

SYN Flag

¿Qué número de secuencia relativo está establecido?

0

¿Cuáles son los valores de los puertos de origen y destino?

80 y 51800

¿Qué marcadores están establecidos?

Acknowledgement Flag y Syn Flag

¿En qué valores están definidos los números de secuencia relativa y confirmación?

Número de secuencia relativo es 0 y del reconocimiento es 1

¿Qué marcadores están establecidos?

Acknowledgement Flag

Los números relativos de secuencia y reconocimiento están establecidos en 1 como punto de inicio. La conexión TCP está establecida, y la comunicación entre el equipo de origen y el servidor web puede comenzar.

¿Qué hace el switch -r?

La opcion -r le permite leer el paquete del archivo que se guardó usando la opcion -w con tcpdump u otras herramientas que escriben archivos pcap o pcap-ng.

Preguntas de reflexión

1. Hay cientos de filtros disponibles en Wireshark. Una red grande podría tener numerosos filtros y muchos tipos diferentes de tráfico. Mencione tres filtros que podrían ser útiles para un administrador de redes.

   TCP, direcciones IP especificas y protocolos HTTPS

2. ¿De qué otras maneras podría utilizarse Wireshark en una red de producción?

   Wireshark se usa a menudo con fines de seguridad para el analisis posterior del trafico normal o despues de un ataque de red.