Notas del 13 oct

Recapitulando protocolos

UDP

No requiere confirmacion de llegada No importa si se dana, pierde o no llega

Como ejemplo en servicios de streaming si no llega un paquete de framos no hace falta re-enviar un paquete perdido porque ya para ese entonces va a llegar otro paquete de frames. Esto se puede percibir cuando se pega el video y despues sigue

TCP/443

Zoom aunque es streaming, que es generalmente asociado a UDP, usa TCP

IANA

Internet Assigned Numbers Authority

Para utilizar formalmente un puerto si se crea un nuevo servicio se tiene que registrar en IANA Puede que alguien lo puede registrar antes, aunque aun se puede usar, comercialmente es complicado

HTTPS es muy constante, todo applicacion que tenga que ver con internet usa HTTPS, por lo que hay una garantia que el puerto TCP/443 se encuentra abierto en todos los firewalls, si se cerrara este puerto no se podria navegar.

Para que una aplicacion tenga un buen alcance se debe usar este puerto, otra ventaja es que este puerto esta encriptado

Abrir puertos no registrados es un dolor de cabeza, por eso todo el mundo usa 443

Capa de transporte

Como siempre, tiene retries y time-outs son especialmente importantes en esta capa, porque aqui se hace el control de congestion

Problema

Router -> Load balancer -> Granja de servidores

El load balancer distribuye a los servidores

Un usuario malisioso puede enviar exploits hacia los servidores

Hasta que el paquete arriva al servidor se puede dar uno cuenta de que es un exploit, dependiendo de la funcionalidad del router

DoS

> Un exploit puede pasar capa 3 y capa 4, uno de los mas comunes en estas capas se conoce como DoS attack

> Consiste en un script que crea un socket en el puerto de un servidor, esta conexion abre un thread que queda en el servidor, sto se repite hasta acabar la capacidad computacional del servidor

> Un router puede llevar un conteo de numero de conexion por IP. i un actor hace mas de 30 conexiones por minuto, se empiezan a hacer drop de coxiones, porque esto indica que no es un usuario regular, se convierte en un firewall de capa 3

> Se puede tambien hacer un tar pit, se hace un delay a cada conexion, en este caso el atacante gasta sus recursos sin lograr llegar al servidor, antes de que cada conexion expira el router lo mantiene vivo

> Se puede hacer un tar pit basado en la ubicacion geografica del IP. Aunque un ataque DoS distribuido es mucho mas dificil de atrapar en capa 3, requiere meter capa 7 en lo que se pueden identificar patrones de URLs y parameters y filtrar en base a eso

Un router puede revisar los paquetes e intentar filtrar exploits. Entre mas alta la capa que maneje mas informacion puede conseguir

Un router de capa 7 va a hacer mas uso de recursos computacionales, por lo que puede hacer que los paquetes sean procesados de forma mas lenta

Los routers mas grandes son solamente capa 3, solo routeo

La capa de transporte da la confiabilidad a la conexion TCP/IP es bastante eficiente

Para saber mas de TCP: https://www.ietf.org/rfc/rfc793.txt

Puede ser orientado a conexion o no

Primitivas

Crea primitivas que abstraen comportamiento que se traduce a capa de red

1. Listen
2. Connect
3. Send
4. Receive
5. Disconnect