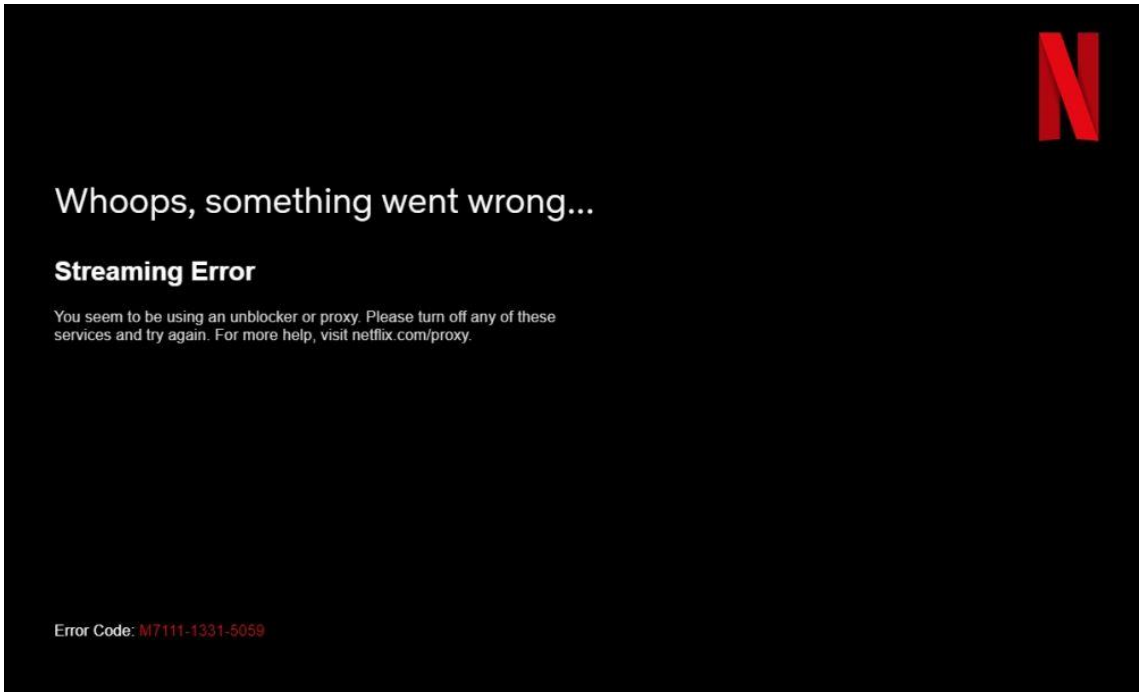
Ejemplo de Desarrollo II

Contenido

Predicción Ataque DDOS

Estado del Arte

Un ataque de denegación de servicios es lo que su nombre indica, que el servidor al que queremos acceder no nos responda. Es decir, que nuestras peticiones o clicks a un capítulo de nuestra serie favorita, por ejemplo “House of Cards” de Netflix, nos expulse o no nos deje acceder a sus contenidos.

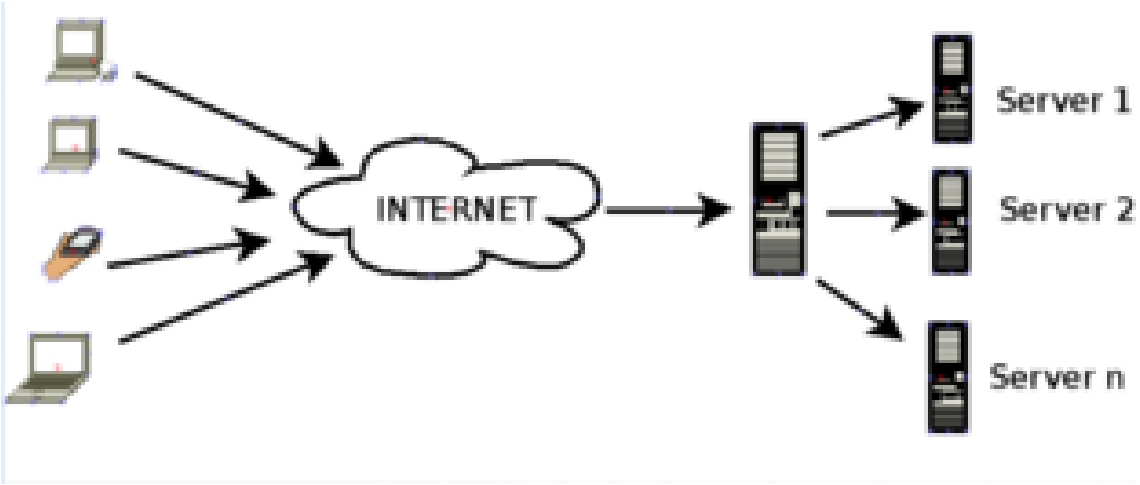


“¡Oye, estoy pagando por un servicio, dádmelo!” – ¿Es lo primero que pensaríamos, cierto?

https://everydaywithtay.files.wordpress.com/2015/02/tumblr_n1bo4ol7v61sikq5fo1_500.gif

La envergadura de un ataque de este tipo es muy grande. Actualmente ya no existe un único servidor al que accede todo el planeta. Suele haber distintos servidores y gestores de paquetería de datos para distribuir toda la circulación de información a los distintos nodos para no sobrecargar e inutilizar ningún servidor. A estos distribuidores se les suele llamar Balanceadores de carga.

Materializando el problema: Casos de uso (vol.2)



¿Un ataque de denegación de servicios distribuido (DDoS) entonces a dónde atacaría? – Exacto, al Balanceador De Cargas.

Una vez que se hayan inutilizado los balanceadores de carga, los servidores quedarían totalmente inutilizables al haber cortado su nodo de comunicación con el exterior. Un ataque de este tipo que encima robe la información de dichos servidores sería ya un mate para dicha empresa.

Hecho este preludio, vayamos a analizar el problema.

Problema / Solución:

Lo que recibiremos de internet es un conjunto de bits en un vector de un tamaño determinado. De esta paquetería nos gustaría registrar también la hora y el flujo de información por minuto. A pesar de ser un conjunto de bits, nos tocaría segmentarlos y separarlos para extraer la información de forma ordenada. Aquí una sugerencia propuesta.

ENTRADA	Hora	IP remitente	IP Destino	Contenido	Protocolo	Nivel de Acceso
SALIDA	Nivel de Acceso	Protocolo	Contenido	IP Destino	IP remitente	Hora

Con este paso, pasaríamos de tener datos desestructurados a ordenarlos para nuestro objetivo, detectar un posible ataque a un balanceador y capar ciertas conexiones.

Para poder extraer dicha información del balanceador de carga utilizaremos un sniffer que, aunque suena muy chulo, no es más que un aparato con forma de router que analiza los paquetes o tramas que entran y salen de internet.

Nosotros simplemente inhalamos esa información. Dichos datos nos la tiene que proporcionar el cliente o dejarnos a nosotros nuestros dispositivos para poder extraerla de forma trasparente.

Una vez hayamos estructurado los datos ya tenemos el paso previo para alimentar nuestro modelo, ya sea de Machine Learning, Deep Learning o un simple clasificador.

Aún nos falta ver las distintas herramientas que usaremos, ya os las dispondremos. De momento simplemente que os suenen.

Para saber si nuestro modelo funciona bien sabiendo si la información que tenemos es suficiente o necesitamos más lo probaríamos con datos de distintas entidades.

Aquí, el acceso a la información sería directa con el cliente ya que es raro que una empresa publique sus datos de flujo de información con IPs de usuarios reales y aún menos información comprometedora respecto a cuándo han o están fallado.

Por tanto, en este ejemplo, no se han adjuntado links a los que poder acceder para extraer dicha información.

Pero no os preocupéis, más adelante simularemos uno de estos ataques a nuestro propio router.

https://qph.fs.quoracdn.net/main-qimg-4fd822d29e11dee8ed4fb26404d911d0

Conclusiones

En este boceto de proyecto había muchas partes a las que desgraciadamente no podremos acceder, esto se vuelve exclusivo de la compañía con la que trabajemos por lo que solo se podía explicar de manera general.

Por lo menos sí habéis visto que es un ataque de negación de servicios y lo que esto puede acarrear. Espero que el ejemplo de acceso a servidores del estilo de Netflix o Tik-Tok sirva como ejemplo de la importancia de la ciberseguridad, una vez más.

No se ha querido indagar en los métodos para comprobar nuestro modelo. Dentro de poco nos pondremos a cómo interpretar los datos y calcular funciones de coste para nuestros modelos personalizados.

De momento solo queremos que vuestra mente empiece a volver información útil cualquier contenido. Este ejercicio es algo más abstracto que los anteriores, pero creemos que es fundamental.

Materializando el problema: Casos de uso (vol.2)
NOTA:

Este es un ejemplo algo más desarrollado para que os hagáis una idea de cómo conceptualizar un problema a la realidad…un boceto. Se ha tratado de hacerlo ameno. De momento no se ha querido hacerlo profesional sino digerible.

Enfoca el documento como mejor lo prefieras, la idea es que la otra persona lo entienda.

La mayoría de los ejercicios propuestos en el volumen 2 son un poco más desarrollados y tienen que ser algo más desarrollados.

Espero que el documento del ejercicio anterior os sirva como plantilla para este.

Ejercicios

Bueno, creo que llego la hora…es tu-turno!

Elige uno de los siguientes temas e intenta desarrollar un ejemplo similar al que se os ha facilitado más arriba. Suerte @eggers!

1. **Análisis de sentimientos en textos**
2. **Detección correos fraudulentos**
3. ~~**Predecir un ataque DDOS(ciberseguridad)**~~
4. **Tomar decisiones sobre donde puede ser interesante poner capital (Acciones en empresas)**
5. **Ayuda a la hora de hacer fotografías (balance de blancos, color, contraste…cómo?)**
6. **Adelantarse a nuestros gustos. Como lo hacen Amazon, Microsoft, Google (General)**
7. **Aumentar calidad de imágenes. Posible uso para servidores más pequeños.**
8. **Recuento de especies de manera no intrusiva Aérea**
9. **Traducir textos de otros idiomas**