PREVENCIÓN DE ATAQUES

Juan Carlos Hermoso Quesada
Alejandro Gallardo Fernández

1.- Introducción

En este trabajo vamos a tratar sobre algunos de los muchos tipos de ataques informáticos (o cibernéticos) que hay. Luego hablaremos más a fondo de los ataques DDoS, ya que son de los que más se escuchan en las noticias y se leen por las redes sociales. Y por último veremos cómo mitigar un ataque DDoS tras su prevención.

Hoy en día prácticamente todo el mundo conoce el significado de un ataque informático y cómo puede perjudicar a nuestra empresa o negocio. Por esa razón, intentamos buscar soluciones para prevenir estos ataques, y para ello, solemos implementar unas medidas en nuestro sistema para que sea lo menos vulnerable posible.

2.- Tipos de vulnerabilidades

Vulnerabilidades generales:

- Metadatos: con ellos es posible conocer nombre de usuario, equipos, SO, versiones de SO... Hasta se puede realizar un mapa interno de la organización (equipos cliente, usuarios, servidores...)
- Configuración débil
- Comunicación insegura cliente y servidor
- Software desactualizado

Vulnerabilidades basadas en RedHat (aplicables a muchas distribuciones de Linux):

- Contraseñas predeterminadas o ninguna: comúnmente asociadas con hardware de redes, por ejemplo, el firewall.
- Llaves compartidas o predeterminadas: si no se cambian las llaves de seguridad predeterminadas, cualquier usuario con esas llaves podrá acceder al cualquier recurso e información de llave compartida.
- Suplantación de IP: acceso desde máquina remota disfrazada de nodo en la red local.

- Interceptación pasiva: recolección de datos pasan entre dos nodos (hecha, por ejemplo, con una suplantación de IP).

3.- Tipos de ataques

Como hemos mencionado antes, vamos a ver en qué consisten algunos de los tipos de ataques informáticos que existen, entre los cuáles podemos encontrar los siguientes:

Ataques de phishing:

Los ataques de phishing se basan en la suplantación de identidad y son unos de los principales ataques de malware y básicamente están compuestos por un archivo adjunto de un correo electrónico. Generalmente estos correos electrónicos se hacen pasar por una empresa legítima.

Son fáciles de detectar ya que suelen tener una alta cantidad de errores gramaticales y ortográficos y tienden a pedir información personal o de crédito cuando, normalmente, dichas empresas no requieren esa información y no suelen redirigir al usuario hacia enlaces externos por correo electrónico.

El instituto InfoSec reconoce 7 tipos de ataques de phishing:

1. Sitios web de phishing
2. Ataques a las redes sociales
3. Spear-Phishing
4. Declaraciones de impuestos fraudulentas
5. Llamadas tlf. Phishy
6. Charity Phishing
7. CEO Phishing

Ataques network-probes:

Los ataques Network-probes consisten en colocar una sonda de red para intentar obtener acceso a una computadora y sus archivos a través de un punto débil ya conocido o muy probable en los sistemas informáticos.

Las sondas de red en si no son una amenaza inmediata. Sin embargo, sí que indican que alguien está instalando en su sistema un programa para posibles puntos de entrada como vector para el ataque. Básicamente es un monitor de red que analiza protocolos y tráfico de red en tiempo real.

- ## Ataques de fuerza bruta:

  Los ataques de fuerza bruta y Cracking son unos métodos de prueba y error utilizado por los programas de aplicación para decodificar datos cifrados como contraseñas o claves de cifrado de datos (DES), utilizando la fuerza bruta, o sea mediante un esfuerzo exhaustivo, en vez de emplear estrategias intelectuales o más sofisticadas.

  El crackeo de la fuerza bruta básicamente consiste en ir introduciendo de manera continua una contraseña tras otra hasta que acierta, lo que permite la entrada al sitio que se está atacando.

- ## Ataques Drive-by download:

  Los ataques Drive-by Download consisten en que un programa se te descarga automáticamente en el dispositivo sin su consentimiento o incluso **con conocimiento pero con desconocimiento.**

  Los ataques Drive-by Download se activan simplemente cuando una víctima hace clic en un enlace que, involuntariamente, inyecta software malicioso en el dispositivo.

  El malware que se usa con más frecuencia en los ataques Drive-by Download se denomina **troyano**.

- ## Ataques de denegación de servicio - DDoS:

  Los ataques de Denegación de servicios distribuidos (DDoS) tratan de intentar que un servicio online no esté disponible al mandarle una enorme cantidad de solicitudes a la vez sometiendo, de esta forma, al servicio, a una sobrecarga con tráfico de múltiples fuentes.

  Los ataques DDoS son uno de los ataques más comunes usados para comprometer el sistema de una organización. Es un ataque que usa múltiples sistemas infectados para apuntar a un solo sistema. Estos sistemas suelen estar infectados con un troyano y se utilizan para colapsar un servicio en línea, lo que afecta a las capacidades de publicar y acceder a información importante.

- Ataques de Amenaza Persistente Avanzada (APT):
  Los ataques APT consisten en un ataque de red en el que un usuario no autorizado obtiene acceso a una red y se queda allí sin que le detecten durante un tiempo prolongado.

  El objetivo de un ataque APT es mantener el acceso encubierto y continuo a una red. Esto permite a los piratas informáticos recopilar continuamente credenciales de usuario válidas y acceder cada vez a más información valiosa.

  Un ataque APT tiene como objetivo recopilar información en lugar de cerrar una red, lo que requiere la reescritura continua de códigos y sofisticadas técnicas de evasión.

- Ataques de ransomware:
  Los ataques de ransomware consisten en un tipo de software malicioso creado para bloquear el acceso a un sistema informático hasta que se pague una suma de dinero.

  El ransomware se está haciendo popular y los piratas informáticos se están dando cuenta de los beneficios financieros de usar estas tácticas. Un ataque ransomware ocurre cuando un hacker infecta un pc o servidor, ya sea con un software malicioso cerrando su sistema (locker-ransomware) o mediante el cifrado personalizado de archivos importantes en el sistema y exigiendo un rescate (generalmente en bitcoins) a cambio de sus sistemas / archivos (crypto-ransomware).

3.1.- Tipos de ataques DDoS

- Syn Flood (Inundación Syn)
  Estos ataques ocurren cuando una persona o programa logra hacerse pasar por otro exitosamente, falsificando datos (spoof). Luego inunda, con paquetes SYN, la tabla de conexión de los servidores, bombardeándolos hasta que los hacen caer. Lo bueno es que son pocos los ataques SYN flood y pueden ser detenidos fácilmente por software de firewalls. Los ataques SYN flood de alto ancho de banda, sin embargo, requieren equipo más especializado con capacidades de proxy SYN.

- Zombie Flood (Inundación Zombi)

  Este ataque ocurre cuando conexiones que no han sido falsificadas sobrecargan los servicios, causando parálisis en la red. A diferencia de los ataques SYN flood, los asaltos Zombie flood son más difíciles de detener a menos que la víctima atacada tenga algún tipo de tecnología de mitigación de comportamiento. Aún más difíciles de controlar son los Zombi floods de alto ancho de banda, las cuales requieren lógica especializada para conexiones legítimas y límite de rango.

- ICMP Flood (Inundación ICMP)

  Este ataque ocurre como resultado de paquetes ICMP que sobrecargan los servidores a tal grado de ocasionar una falla en el sistema. Un volumen bajo de ataques ICMP flood puede ser detenido fácilmente con Listas de Control de Acceso (ACLs por sus siglas en inglés) en los ruteadores y switches. Como otros ataques de ancho de banda alto, los ICMP flood de alto ancho de banda, necesitan de equipo especializado.

- Inundación de Puertos Fuera de Servicio (Non-service Port Flood)

  En este ataque, paquetes TCP/UDP bombardean los servidores, elevando el flujo de tráfico en servidores sin uso. Las organizaciones pueden combatir fácilmente este tipo de ataques con ACLs, pero ataques más poderosos requieren de soluciones de seguridad más fuertes.

- Inundación de Puertos de Servicio (Service Port Flood)

  En este tipo de ataques, los paquetes bombardean los puertos en servicio que ya habilitan el tráfico pesado (como por ejemplo el puerto TCP 80) hacia y desde la red de la organización. Estos tipos de ataques son de los más traicioneros debido al hecho de que no se pueden detener o desacelerar por muchas de las soluciones estándares de seguridad y de red – incluyendo *firewalls*, *switches*, dispositivos IPS y ruteadores. Para bloquear estas amenazas las organizaciones deberán invertir en tecnologías de seguridad más sofisticadas.

- Fragment Flood (Inundación fragmentada)

  Como su nombre sugiere, este tipo de ataque ocurre cuando paquetes fragmentados sobrecargan los servidores. Como en los ataques de inundación de puertos de servicio, los ataques por inundación fragmentada no pueden ser frustrados con el esquema estándar de *firewalls, switches* y ruteadores. En cambio, éstos requieren soluciones más robustas para detenerlos de raíz.

- HTTP GET Flood (Inundación HTTP GET)

  Este tipo de ataque resulta de *bots* orientados a las conexiones que inundan los servidores afectando el tráfico de la red en puertos de servicio como el HTTP, mientras se hacen pasar por usuarios legítimos. Los firewalls, switches y ruteadores tampoco los detendrán. Para hacerlo, la organización víctima deberá reforzar su estructura de seguridad con soluciones más resistentes.

- Blended Flood (Inundación Mezclada)

  Esto se da cuando múltiples tipos de ataques se combinan en el servidor, lo cual al final termina confundiendo al equipo. Debido a su complejidad, no pueden ser detenidos con facilidad por firewalls, switches, ruteadores, ni dispositivos IPS.

- Anomalous Packet Flood (Inundación de Paquetes Anómalos)

  En ese tipo de ataque, paquetes con encabezados o estado anómalos sobrecargan los servidores y ahogan la red. Sin embargo, las organizaciones pueden aprovechar algunos firewalls y dispositivos IPS para detener estos ataques. Para tal fin, las soluciones diseñadas para detectar y proteger las redes de asaltos DDoS pueden fácilmente detener este tipo de ataques.

- Inundación de una Región Foránea

  Esto ocurre cuando *bots* de una específica región geográfica atacan los servidores de la organización víctima. Este tipo de ataques son usualmente generados a través de campañas dirigidas muy completas, y como tales, son usualmente más difíciles de reprimir. Entre otras cosas, los equipos de seguridad diseñados para combatir estos ataques necesitarán contener tecnologías de visibilidad con la habilidad de detectar automáticamente patrones de comportamiento irregulares o anómalos.

4.- Tipos de prevenciones de ataques

- Alerta temprana: mediante, por ejemplo, la monitorización. Con el siguiente comando, podemos monitorizar todas las IPs que están conectadas en el puerto 80 (web) junto con el número de peticiones realizadas ordenadas de mayor a menor.

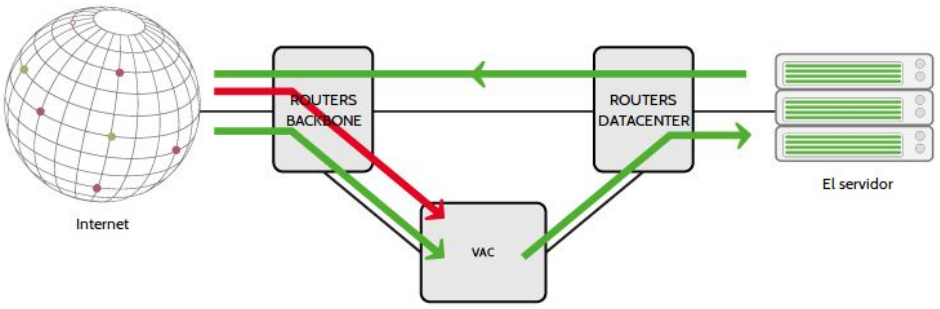
  netstat -tn 2>/dev/null | grep :80 | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -nr | head

- Provisión de ancho de banda: disponer de un ancho de banda teóricamente mayor al necesitado. De esta manera, lograremos una acomodación mayor del tráfico inesperado y tendremos más tiempo de reacción a la hora de lidiar con los ataques.

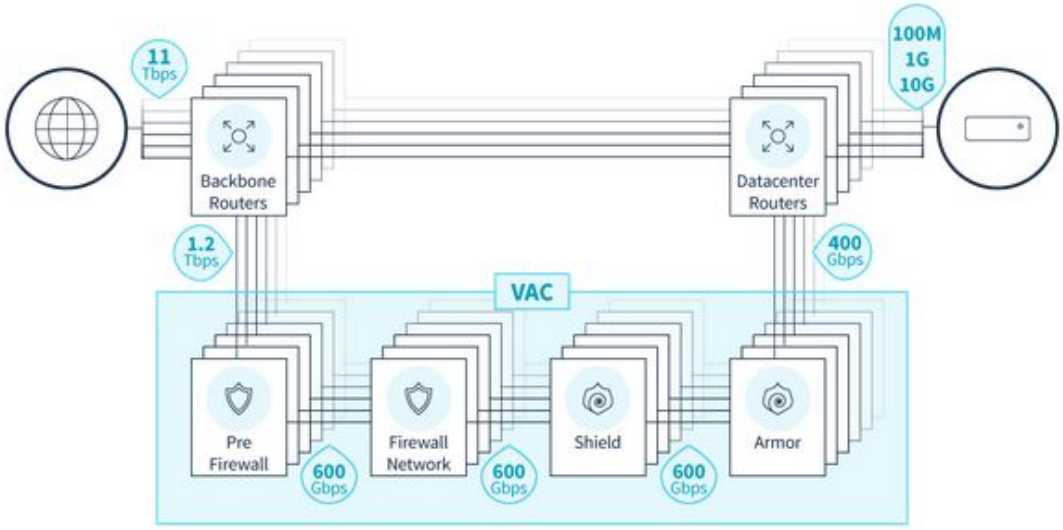
- Defender el perímetro de red:
  - Limitaciones en el router acceso
  - Filtros de descarte de fuentes atacantes ya identificadas
  - Reducir el timeout de conexiones abiertas de manera agresiva

- Llamar a nuestro proveedor de servicios de internet o de hosting

- Mitigación DDoS: cuando el DDoS ya está en proceso, lo mejor es realizar una mitigación, que lo que hace es que redirigir el tráfico atacante hacia una red de filtros, de manera que todo el tráfico pasa por la red de filtros, en el cual se queda parte del tráfico que es ilegítimo mientras que se deja pasar el tráfico legítimo hacia el servidor.



La red de filtros suele ser una red multicapa, en el cual se encuentran varios dispositivos encargados de dicha filtración. La siguiente imagen esquematiza la red de filtros del servicio anti-DDoS de la empresa OVH:



- Pre Firewall: conjunto de switches que enruta el tráfico en las siguientes etapas. Permite el acceso de los protocolos TCP, UDP, ICMP y GRE y bloquea los demás.

- Firewall Network: conjunto de tres routers virtuales que permite clasificar el tráfico mediante reglas (listas de acceso) configurables y modificables.

- Shield: conjunto de tres routers virtuales encargados de mitigar ataques conocidos, especialmente los que funcionan por amplificación.

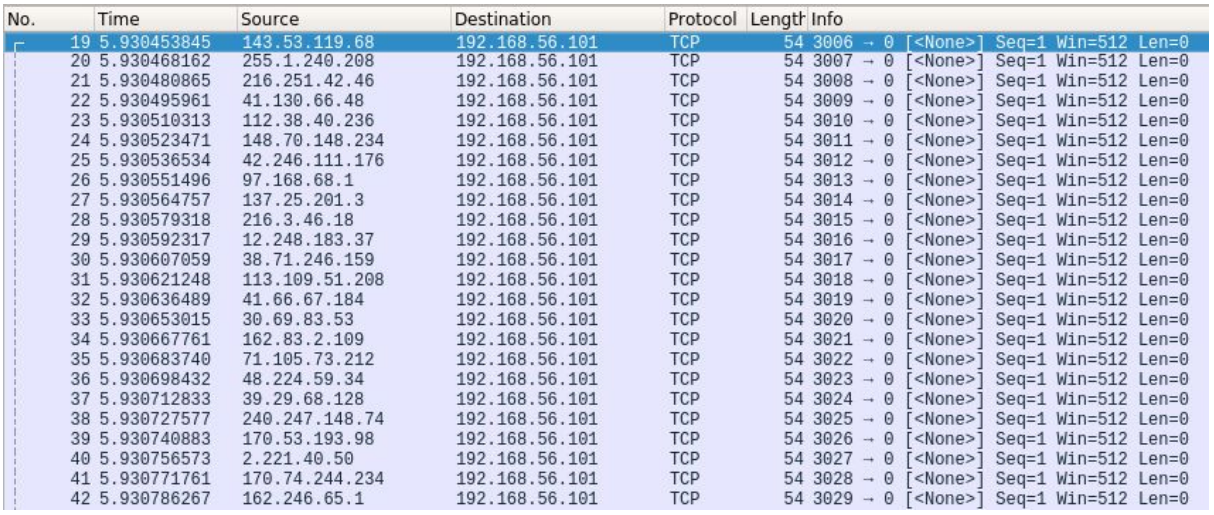
- Armor: conjunto de tres routers virtuales encargados de mitigar los ataques más sofisticados.

5.- Demostración práctica de una prevención contra un DDoS

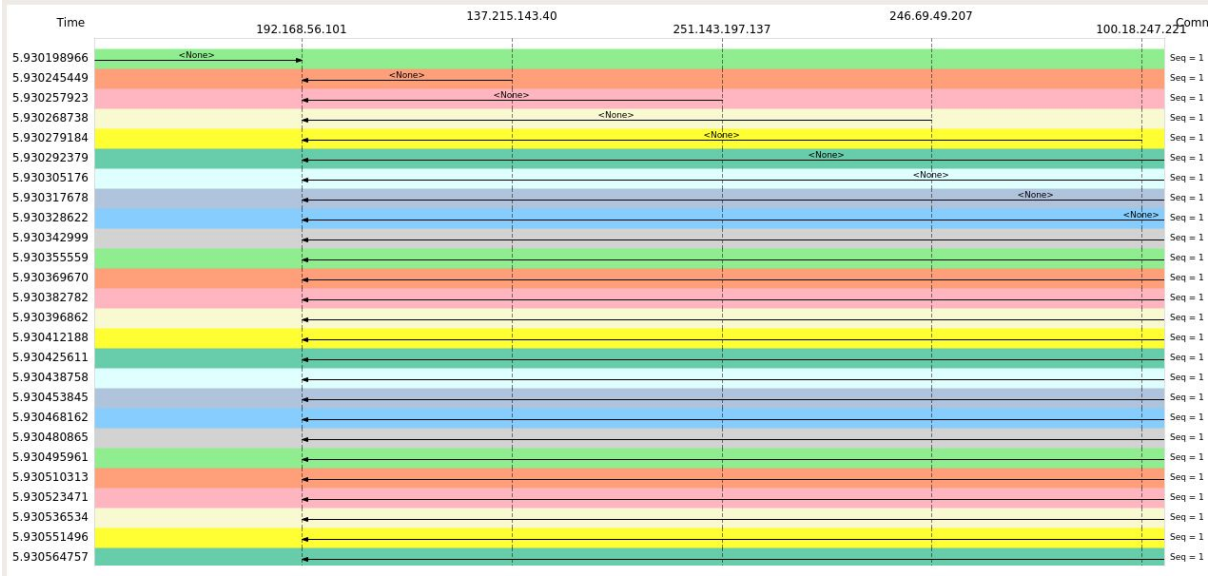
Para la demostración práctica, hemos realizado la simulación de un ataque DDoS (SYN flood) y su correspondiente mitigación.

Mediante el comando **hping3** podemos realizar peticiones masivas mediante el parámetro **--flood** y desde fuentes desconocidas modificando la IP de origen mediante el parámetro **--rand-source**.

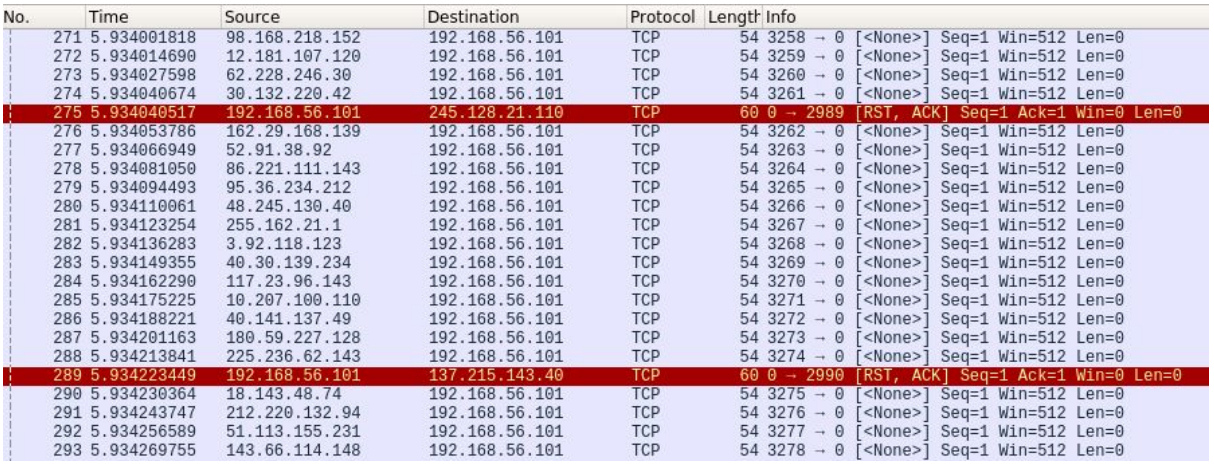
Teniendo en cuenta que la máquina (virtual) servidora víctima tiene como IP **192.168.56.101**, realizando el comando **hping3 --rand-source --flood 192.168.56.101** y parándolo al segundo podemos ver el tráfico de paquetes usando Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
19	5.930453845	143.53.119.68	192.168.56.101	TCP	54	3006 → 0 [<None>] Seq=1 Win=512 Len=0
20	5.930468162	255.1.240.208	192.168.56.101	TCP	54	3007 → 0 [<None>] Seq=1 Win=512 Len=0
21	5.930480865	216.251.42.46	192.168.56.101	TCP	54	3008 → 0 [<None>] Seq=1 Win=512 Len=0
22	5.930495961	41.130.66.48	192.168.56.101	TCP	54	3009 → 0 [<None>] Seq=1 Win=512 Len=0
23	5.930510313	112.38.40.236	192.168.56.101	TCP	54	3010 → 0 [<None>] Seq=1 Win=512 Len=0
24	5.930523471	148.70.148.234	192.168.56.101	TCP	54	3011 → 0 [<None>] Seq=1 Win=512 Len=0
25	5.930536534	42.246.111.176	192.168.56.101	TCP	54	3012 → 0 [<None>] Seq=1 Win=512 Len=0
26	5.930551496	97.168.68.1	192.168.56.101	TCP	54	3013 → 0 [<None>] Seq=1 Win=512 Len=0
27	5.930564757	137.25.201.3	192.168.56.101	TCP	54	3014 → 0 [<None>] Seq=1 Win=512 Len=0
28	5.930579318	216.3.46.18	192.168.56.101	TCP	54	3015 → 0 [<None>] Seq=1 Win=512 Len=0
29	5.930592317	12.248.183.37	192.168.56.101	TCP	54	3016 → 0 [<None>] Seq=1 Win=512 Len=0
30	5.930607059	38.71.246.159	192.168.56.101	TCP	54	3017 → 0 [<None>] Seq=1 Win=512 Len=0
31	5.930621248	113.109.51.208	192.168.56.101	TCP	54	3018 → 0 [<None>] Seq=1 Win=512 Len=0
32	5.930636489	41.66.67.184	192.168.56.101	TCP	54	3019 → 0 [<None>] Seq=1 Win=512 Len=0
33	5.930653015	30.69.83.53	192.168.56.101	TCP	54	3020 → 0 [<None>] Seq=1 Win=512 Len=0
34	5.930667761	162.83.2.109	192.168.56.101	TCP	54	3021 → 0 [<None>] Seq=1 Win=512 Len=0
35	5.930683740	71.105.73.212	192.168.56.101	TCP	54	3022 → 0 [<None>] Seq=1 Win=512 Len=0
36	5.930698432	48.224.59.34	192.168.56.101	TCP	54	3023 → 0 [<None>] Seq=1 Win=512 Len=0
37	5.930712833	39.29.68.128	192.168.56.101	TCP	54	3024 → 0 [<None>] Seq=1 Win=512 Len=0
38	5.930727577	240.247.148.74	192.168.56.101	TCP	54	3025 → 0 [<None>] Seq=1 Win=512 Len=0
39	5.930740883	170.53.193.98	192.168.56.101	TCP	54	3026 → 0 [<None>] Seq=1 Win=512 Len=0
40	5.930756573	2.221.40.50	192.168.56.101	TCP	54	3027 → 0 [<None>] Seq=1 Win=512 Len=0
41	5.930771761	170.74.244.234	192.168.56.101	TCP	54	3028 → 0 [<None>] Seq=1 Win=512 Len=0
42	5.930786267	162.246.65.1	192.168.56.101	TCP	54	3029 → 0 [<None>] Seq=1 Win=512 Len=0



Como podemos ver, en menos de una milésima de segundo, se mandan muchos paquetes desde direcciones desconocidas, a las cuales el servidor intenta contestar pero sin poder dar a basto



No.	Time	Source	Destination	Protocol	Length	Info
271	5.934001818	98.168.218.152	192.168.56.101	TCP	54	3258 → 0 [<None>] Seq=1 Win=512 Len=0
272	5.934014690	12.181.107.120	192.168.56.101	TCP	54	3259 → 0 [<None>] Seq=1 Win=512 Len=0
273	5.934027598	62.228.246.30	192.168.56.101	TCP	54	3260 → 0 [<None>] Seq=1 Win=512 Len=0
274	5.934040674	30.132.220.42	192.168.56.101	TCP	54	3261 → 0 [<None>] Seq=1 Win=512 Len=0
275	5.934040517	192.168.56.101	245.128.21.110	TCP	60	0 → 2989 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
276	5.934053786	162.29.168.139	192.168.56.101	TCP	54	3262 → 0 [<None>] Seq=1 Win=512 Len=0
277	5.934066949	52.91.38.92	192.168.56.101	TCP	54	3263 → 0 [<None>] Seq=1 Win=512 Len=0
278	5.934081050	86.221.111.143	192.168.56.101	TCP	54	3264 → 0 [<None>] Seq=1 Win=512 Len=0
279	5.934094493	95.36.234.212	192.168.56.101	TCP	54	3265 → 0 [<None>] Seq=1 Win=512 Len=0
280	5.934110061	48.245.130.40	192.168.56.101	TCP	54	3266 → 0 [<None>] Seq=1 Win=512 Len=0
281	5.934123254	255.162.21.1	192.168.56.101	TCP	54	3267 → 0 [<None>] Seq=1 Win=512 Len=0
282	5.934136283	3.92.118.123	192.168.56.101	TCP	54	3268 → 0 [<None>] Seq=1 Win=512 Len=0
283	5.934149355	40.30.139.234	192.168.56.101	TCP	54	3269 → 0 [<None>] Seq=1 Win=512 Len=0
284	5.934162290	117.23.96.143	192.168.56.101	TCP	54	3270 → 0 [<None>] Seq=1 Win=512 Len=0
285	5.934175225	10.207.100.110	192.168.56.101	TCP	54	3271 → 0 [<None>] Seq=1 Win=512 Len=0
286	5.934188221	40.141.137.49	192.168.56.101	TCP	54	3272 → 0 [<None>] Seq=1 Win=512 Len=0
287	5.934201163	180.59.227.128	192.168.56.101	TCP	54	3273 → 0 [<None>] Seq=1 Win=512 Len=0
288	5.934213841	225.236.62.143	192.168.56.101	TCP	54	3274 → 0 [<None>] Seq=1 Win=512 Len=0
289	5.934223449	192.168.56.101	137.215.143.40	TCP	60	0 → 2990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
290	5.934230364	18.143.48.74	192.168.56.101	TCP	54	3275 → 0 [<None>] Seq=1 Win=512 Len=0
291	5.934243747	212.220.132.94	192.168.56.101	TCP	54	3276 → 0 [<None>] Seq=1 Win=512 Len=0
292	5.934256589	51.113.155.231	192.168.56.101	TCP	54	3277 → 0 [<None>] Seq=1 Win=512 Len=0
293	5.934269755	143.66.114.148	192.168.56.101	TCP	54	3278 → 0 [<None>] Seq=1 Win=512 Len=0

Nuestra mitigación consiste en una limitación del número de paquetes por segundo

sudo iptables -A INPUT -m state --state RELATED,ESTABLISHED -m limit --limit 50/second --limit-burst 50 -j ACCEPT

De manera que las peticiones no podrán superar las cincuenta por segundo. En el caso de que lo superen, el DDoS se verá anulado. Como el comando hping3 lanza muchas peticiones por milésima de segundo, el DDoS de esta forma resulta imposible.

6.- Referencias

1. https://www.ovh.es/anti-ddos/gestion-ataques-ddos.xml
2. https://www.ovh.es/anti-ddos/principio-anti-ddos.xml
3. https://www.ovh.es/anti-ddos/consejos-de-proteccion.xml
4. https://ciberseguridad.blog/algunos-tipos-de-ataques-informaticos/
5. https://mundocontact.com/los-10-tipos-de-ataques-ddos-mas-comunes/
6. https://seohacks.es/ddos/
7. https://www.ovh.es/anti-ddos/mitigacion.xml
8. https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-common_exploits_and_attacks
9. https://www.youtube.com/watch?v=SbUZpyQk-a0
10. https://www.ovh.es/anti-ddos/pre-firewall.xml
11. https://www.ovh.es/anti-ddos/firewall-network.xml
12. https://www.ovh.es/anti-ddos/shield.xml
13. https://www.ovh.es/anti-ddos/armor.xml
14. http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-iptables-options.html