Daniel Ubalde

danielubaldelaguia@gmail.com

Descripción breve

Curso de especialización en ciberseguridad 2022

Caso de uso DDoS



[1. Descripción 2](#_Toc128257924)

[1.1 Tipos de ataques DDoS 3](#_Toc128257925)

[1.1.1 Ataques volumétricos 3](#_Toc128257926)

[1.1.2 Asimétricos 3](#_Toc128257927)

[1.1.3 Computacional 3](#_Toc128257928)

[1.1.4 Basado en la vulnerabilidad 4](#_Toc128257929)

[2. Técnicas relacionadas MITRE 5](#_Toc128257930)

[2.1 T1498/001 Direct Network Flood 5](#_Toc128257931)

[2.2 T1498/002 Reflection Amplification 5](#_Toc128257932)

[3. Detección 6](#_Toc128257933)

[3.1 Una excesiva latencia de la página 6](#_Toc128257934)

[3.2 Monitorizar el tráfico 6](#_Toc128257935)

[3.3 Conexiones sospechosas 6](#_Toc128257936)

[3.4 Acaparamiento de recursos 6](#_Toc128257937)

[4. Fuentes de datos 7](#_Toc128257938)

[4.1 Tráfico de red anormal 7](#_Toc128257939)

[4.2 Registro de eventos del servidor 7](#_Toc128257940)

[4.3 Alertas de seguridad 7](#_Toc128257941)

[4.4 Análisis de paquetes 7](#_Toc128257942)

[4.5 Informes de terceros 7](#_Toc128257943)

[4.6 Monitorización de recursos 8](#_Toc128257944)

[5. Fuentes 9](#_Toc128257945)

# Descripción

Se plantea el caso de un ataque DDoS a la sede de Bionica Automations.

En la sede de Bionica Automations hay servicios cruciales para las operaciones de la empresa y proveer servicios a los clientes.

El objetivo de este caso de uso es analizar los servicios expuestos de la empresa susceptibles a un ataque de DDoS y mitigar sus sonsecuencias.

## Tipos de ataques DDoS

### Ataques volumétricos

Un ataque basado en volúmenes que puede estar en la capa 3, 4 o 7. Los ataques en L3-4 suelen ser tráfico UDP falsificado.

El tipo clásico de DDoS, estos ataques utilizan métodos para generar grandes volúmenes de tráfico y saturar por completo el ancho de banda, creando un atasco de tráfico que hace imposible que el tráfico legítimo fluya hacia dentro o fuera del sitio objetivo.

#### Ataques a las capas de protocolo y transporte (capas 3/4)

Estas herramientas utilizan protocolos como UDP para enviar grandes volúmenes de tráfico a un servidor de destino, por ejemplo, durante una inundación UDP. Estos ataques no suelen ser efectivos de forma individual, por lo que suelen realizarse como ataques DDoS, de manera que su efecto aumenta cuantos más equipos de ataque se usen.

#### Ataques lentos

Tal como su nombre indica, estos tipos de herramientas de ataque usan un volumen bajo de datos y operan muy lentamente. Están diseñadas para enviar pequeñas cantidades de datos a través de múltiples conexiones, para poder mantener abiertos los puertos del servidor objetivo todo el tiempo que sea posible. Además, siguen usando los recursos del servidor hasta impedir que este pueda mantener conexiones adicionales. En particular, estos ataques pueden ser, en ocasiones, efectivos incluso cuando no se utiliza un sistema distribuido como una botnet y con frecuencia los realiza un solo equipo.

### Asimétricos

Los atacantes asimétricos suelen enviar una gran cantidad de paquetes UDP maliciosos a la víctima, inundando el ancho de banda de la red y provocando una denegación de servicio. Además, los atacantes pueden falsificar la dirección IP de origen de los paquetes UDP, lo que hace que la víctima no pueda identificar la fuente real del ataque.

### Computacional

Ataque diseñado para consumir CPU y memoria, generalmente en L7 a través de TCP.

#### Ataques contra la capa de aplicación (capa 7):

Se dirigen contra la capa 7 del modelo OSI, donde se realizan solicitudes basadas en Internet tales como HTTP. Mediante un ataque de inundación HTTP para saturar al servidor objetivo con solicitudes HTTP GET y POST, un actor malintencionado puede lanzar un ataque de tráfico que sea difícil de distinguir de las solicitudes normales que realizan los visitantes reales.

### Basado en la vulnerabilidad

La razón por la que estos ataques son particularmente peligrosos es que aprovechan debilidades específicas del sistema, lo que significa que son difíciles de prevenir y pueden ser muy efectivos. Además, los ataques pueden ser extremadamente dañinos para la reputación de una empresa, ya que pueden hacer que sus servicios sean inaccesibles para los clientes.

# Técnicas relacionadas MITRE

## T1498/001 Direct Network Flood

Los adversarios pueden intentar causar una denegación de servicio (DoS) enviando directamente un alto volumen de tráfico de red a un objetivo. Este ataque DoS también puede reducir la disponibilidad y funcionalidad del sistema(s) y la red objetivo. Las inundaciones directas de red ocurren cuando uno o más sistemas se utilizan para enviar un alto volumen de paquetes de red hacia la red del servicio objetivo. Casi cualquier protocolo de red puede ser utilizado para inundar. Los protocolos sin estado, como UDP o ICMP, son comúnmente utilizados, pero también se pueden utilizar protocolos con estado, como TCP.

Los botnets son comúnmente utilizados para llevar a cabo ataques de inundación de red contra redes y servicios. Grandes botnets pueden generar una cantidad significativa de tráfico desde sistemas repartidos por Internet. Los adversarios pueden tener los recursos para construir y controlar su propia infraestructura de botnet o pueden alquilar tiempo en una botnet existente para realizar un ataque. En algunos de los peores casos de DoS distribuidos (DDoS), se utilizan tantos sistemas para generar la inundación que cada uno solo necesita enviar una pequeña cantidad de tráfico para producir suficiente volumen para saturar la red objetivo. En tales circunstancias, distinguir el tráfico de DDoS de los clientes legítimos se vuelve extremadamente difícil. Las botnets han sido utilizadas en algunos de los ataques de inundación DDoS más destacados, como la serie de incidentes de 2012 que afectaron a importantes bancos de EE. UU.

## T1498/002 Reflection Amplification

Los adversarios pueden intentar causar una denegación de servicio (DoS) reflejando un alto volumen de tráfico de red hacia un objetivo. Este tipo de DoS de red aprovecha un servidor intermediario que aloja y responderá a una dirección IP de origen falsificada. Este servidor de tercera parte se conoce comúnmente como reflector. Un adversario logra un ataque de reflexión enviando paquetes a los reflectores con la dirección falsificada de la víctima. Al igual que en las inundaciones directas de red, se pueden utilizar más de un sistema para llevar a cabo el ataque, o se puede utilizar una botnet. Del mismo modo, se pueden utilizar uno o varios reflectores para concentrar el tráfico en el objetivo. Este tipo de ataque DoS de red también puede reducir la disponibilidad y funcionalidad del sistema (s) y la red objetivo.

Los ataques de reflexión a menudo aprovechan los protocolos con respuestas más grandes que las solicitudes para amplificar su tráfico, comúnmente conocidos como ataques de amplificación de reflexión. Los adversarios pueden generar un aumento en el volumen de tráfico de ataque que es varias órdenes de magnitud mayor que las solicitudes enviadas a los amplificadores. La magnitud de este aumento dependerá de muchas variables, como el protocolo en cuestión, la técnica utilizada y los servidores amplificadores que realmente producen la amplificación en el volumen de ataque. Dos protocolos prominentes que han permitido las inundaciones de amplificación de reflexión son DNS y NTP, aunque se han documentado varios otros en la naturaleza. En particular, el protocolo de memoria caché demostró ser un protocolo potente, con tamaños de amplificación de hasta 51,200 veces el paquete solicitado.

# Detección

## Una excesiva latencia de la página

Una de las formas más comunes de saber que estamos siendo víctimas de un ataque DDoS es que haya una excesiva latencia de la página. Esto significa que los navegadores de los usuarios finales y los servidores responden de manera lenta, hay mucho retraso en la carga y a la hora de navegar por el sitio.

Si esto ocurre podríamos estar ante un ataque de este tipo que esté provocando un mal funcionamiento de la página. Esto nos obligará a tomar medidas para conseguir que todo vuelva a funcionar correctamente.

## Monitorizar el tráfico

También podemos detectarlo gracias a monitorizar el tráfico web. Podemos tener un registro de todo el tráfico y cómo actúa. De esta forma podremos encontrar problemas, entradas de tráfico inusuales, que puedan indicar que estamos ante un ataque DDoS.

Es posible además monitorizar el periodo de impacto y con qué frecuencia se repite lo mismo dentro de un tiempo en concreto. Siempre conviene utilizar programas y servicios que nos ayude a obtener más información sobre la conexión y detectar picos de tráfico inusual.

## Conexiones sospechosas

Una muestra más es cuando vemos un usuario en concreto que está las 24 horas del día enviando solicitudes cada cierto tiempo, que suele ser unos pocos segundos. Esta sería una indicación de que podemos estar sufriendo un ataque DDoS, aunque no se refleje en un mal funcionamiento.

En esta ocasión va a ser interesante también monitorizar la red y el tráfico. Esto es lo que nos indicará que hay algún usuario concreto que no debería estar y que hace saltar las alarmas.

## Acaparamiento de recursos

Podemos verificar también cualquier comportamiento sospechoso con tráfico desconocido hacia nuestro dispositivo o servidor. Al verificar las cargas de tráfico, la cantidad de uso de CPU y el tiempo que puede demorar en dar servicio puede ser un indicio a tener en cuenta.

Siempre que encontremos que hay un consumo excesivo, algo que no suele ser lo habitual, podríamos dudar de si estamos ante un ataque DDoS que está derivando tráfico sospechoso.

# Fuentes de datos

## Tráfico de red anormal

Los sistemas de detección de intrusiones de red (NIDS) y los sistemas de prevención de intrusiones de red (NIPS) pueden detectar y alertar a los administradores de red sobre patrones de tráfico anormal y aumentos de tráfico entrante, lo que podría indicar un posible ataque DDoS.

## Registro de eventos del servidor

Los sistemas de gestión de registros (SIEM) pueden ser configurados para analizar y alertar sobre eventos del servidor específicos, como un aumento en las conexiones activas, solicitudes por segundo o el uso de recursos del sistema, lo que puede indicar un ataque DDoS en curso.

## Alertas de seguridad

Las herramientas de seguridad y monitoreo que envían alertas pueden ser parte de una solución de seguridad integrada que incluya sistemas de detección de intrusiones, firewalls, SIEM y otros sistemas de seguridad.

## Análisis de paquetes

Los sistemas de análisis de paquetes, como Wireshark, pueden utilizarse para analizar el tráfico de red en busca de patrones de ataque DDoS y otros tipos de tráfico malicioso.

## Informes de terceros

Las organizaciones pueden utilizar servicios de inteligencia de amenazas o monitorear fuentes de noticias y foros de seguridad para obtener información sobre actividades de ataque DDoS en curso y alertar a los administradores de seguridad para que tomen medidas preventivas.

## Monitorización de recursos

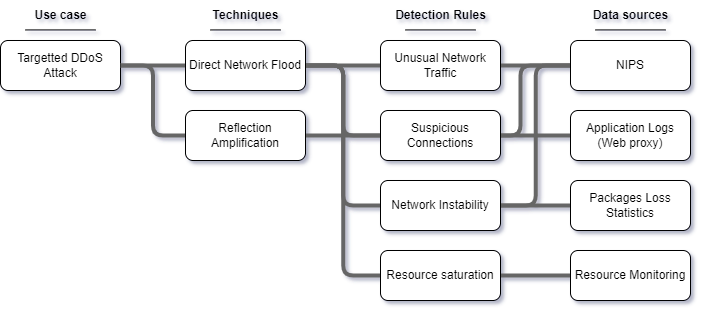
La monitorización de recursos de hardware es esencial para garantizar que los servidores no se sobrecarguen durante un ataque DDoS. Los ataques DDoS pueden ser muy intensivos en recursos y pueden causar el agotamiento de los recursos del servidor, lo que puede provocar un tiempo de inactividad del servicio.

Algunos de los recursos de hardware más importantes que se deben monitorear durante un ataque DDoS son:

1. Uso de CPU: La CPU es el cerebro del servidor y su uso puede indicar si el servidor está sobrecargado o no. Durante un ataque DDoS, la carga en la CPU puede aumentar significativamente, lo que puede reducir el rendimiento del servidor y hacer que se detenga.
2. Uso de memoria: La memoria del sistema es otro recurso importante que se debe monitorear durante un ataque DDoS. Si un ataque DDoS consume demasiada memoria, puede provocar una disminución en el rendimiento del servidor o incluso un bloqueo completo.
3. Uso de disco: El uso de disco también debe ser monitoreado durante un ataque DDoS. Si el disco se satura, puede provocar una disminución en el rendimiento del servidor y hacer que se detenga.

Para monitorear estos recursos de hardware, los administradores de sistema pueden utilizar herramientas de monitorización como Nagios, Zabbix o PRTG Network Monitor. Estas herramientas pueden alertar a los administradores de sistema cuando se detecta un uso elevado de CPU, memoria o disco, lo que puede indicar un posible ataque DDoS en curso. También es importante contar con una infraestructura adecuada, como servidores redundantes y balanceadores de carga, para garantizar que la carga de los servidores se distribuya de manera uniforme y se pueda mitigar el impacto de un posible ataque DDoS.

# Diagrama



# Fuentes

<https://cybersecurity.att.com/blogs/security-essentials/types-of-ddos-attacks-explained>

<https://www.cloudflare.com/es-es/learning/ddos/ddos-attack-tools/how-to-ddos/>

<https://www.redeszone.net/tutoriales/seguridad/reconocer-ataque-ddos/>

<https://www.f5.com/es_es/services/resources/white-papers/the-f5-ddos-protection-reference-architecture>

<https://attack.mitre.org/techniques>