**Ataques Digitales**

<https://www.digitalattackmap.com/>

Debemos saber que si levantamos una aplicación en producción, será atacada de todas maneras. A veces, el ataque puede producirse a los pocos segundos de levantada en el servidor.

Habitualmente un hacker profesional no ataca directamente desde su propia computadora a una organización. Por ejemplo, si quiere atacar Microsoft, no va a atacar desde su computadora sino que pasan sus ataques por diferentes DNS y esos DNS son directamente de países geopolíticamente enemigos.

Los puertos utilizados generalmente para los ataques son el 80, 443 y 53

Puerto 80 (HTTP):

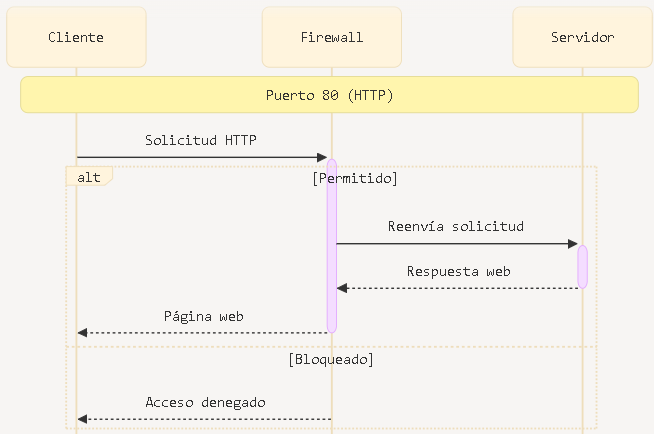
* Utilizado para el tráfico web normal (no seguro)
* Transmite páginas web y contenido HTTP
* Es el puerto predeterminado cuando visitas sitios web sin especificar puerto

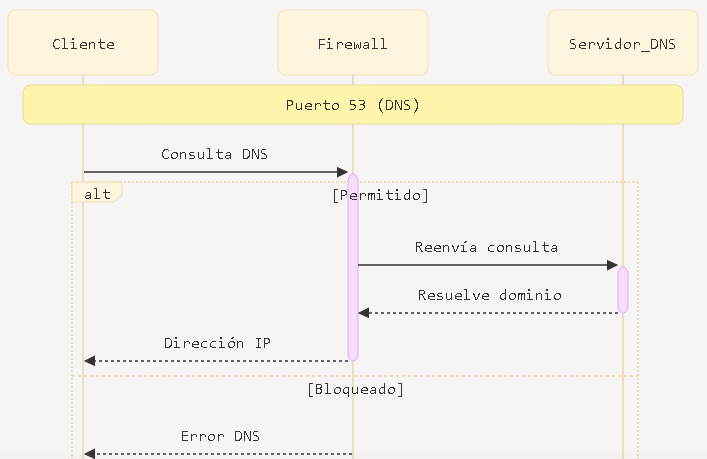
Puerto 443 (HTTPS):

* Utilizado para el tráfico web seguro y encriptado
* Protege la información sensible como contraseñas y datos personales
* Se activa cuando ves "https://" al inicio de una URL

Puerto 53 (UDP/TCP):

* Es el puerto estándar para consultas DNS
* Se usa tanto para UDP como TCP
* Maneja la mayoría de las consultas DNS normales





**Tipos de ataques DDoS (Denegación de Servicio Distribuido)**

Ataque Smurf

Un ataque que explota redes mal configuradas para amplificar el tráfico

Funciona enviando paquetes ICMP con la dirección del objetivo como origen

La red retransmite estos paquetes a todos los dispositivos, creando un efecto multiplicador de hasta 255 veces el tráfico original

Ataque Teardrop

Un ataque que explota vulnerabilidades en la reconstrucción de paquetes TCP/IP fragmentados

Envía paquetes fragmentados diseñados para superponerse entre sí

Cuando el sistema intenta reensamblarlos, los paquetes sobrepuestos causan una falla en el servidor

Ping of Death (POD)

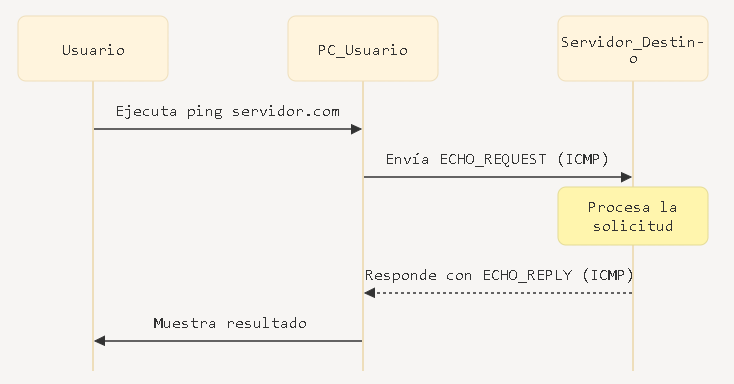
Un ataque que envía paquetes ICMP malformados o excesivamente grandes

Los paquetes exceden el límite máximo permitido de 65,536 bytes

Esto puede causar que el sistema objetivo se bloquee, se inestabilice o se reinicie

**Nota**: Los paquetes ICMP (Internet Control Message Protocol) son mensajes especiales de control que se utilizan en Internet para comunicación entre dispositivos cuando ocurren situaciones específicas o problemas de red.

Para entender mejor cómo funcionan los paquetes ICMP, veamos un ejemplo práctico del proceso más común: el comando ping:



Se utilizan principalmente para:

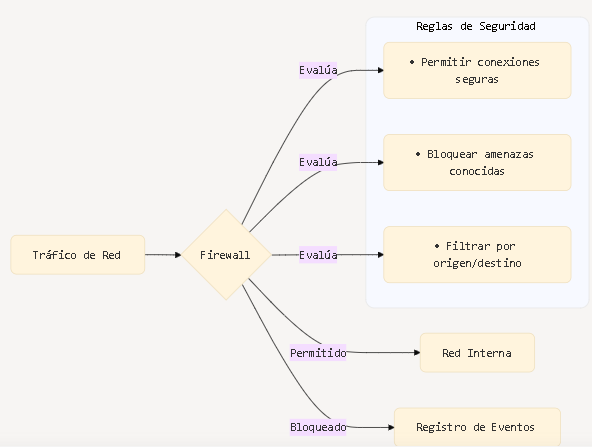
* Confirmar si un dispositivo está conectado (ping)
* Reportar errores de red
* Informar sobre cambios en las rutas de red
* Medir tiempos de respuesta

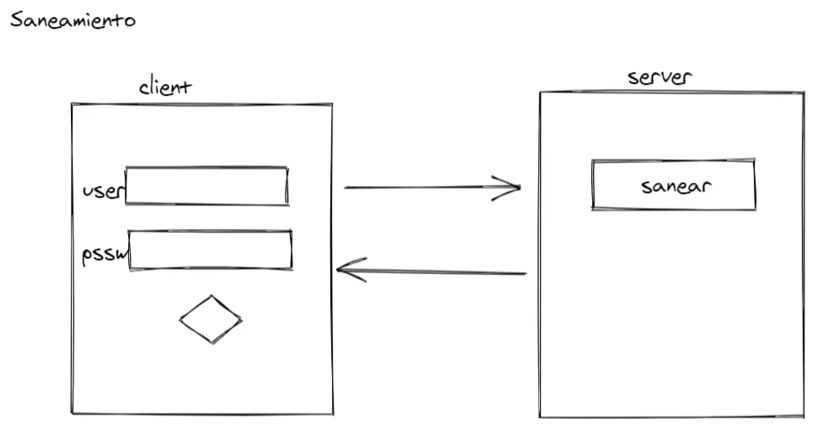
**Firewall**

Los firewalls actúan como guardianes de seguridad que controlan todo el tráfico de red que entra y sale de un sistema o red. Funcionan como una barrera de protección que examina cada paquete de datos y decide si debe permitir su paso o bloquearlo según reglas predefinidas.

Protegen contra ataques maliciosos como los que mencionamos anteriormente (Smurf, Teardrop, Ping of Death)

* Filtran paquetes ICMP sospechosos o no deseados
* Controlan qué aplicaciones pueden comunicarse con Internet
* Mantienen un registro de intentos de intrusión detectados





Sanear una entrada implica que comprobemos los datos que están enviándonos desde el cliente a nuestra aplicación web para comprobar que no hay ningún tipo de hacking o ningún tipo de actividad maliciosa en ese envío de información.

Puede ser que nuestro cliente tenga unos formularios que representan una entrada de datos. Enviamos a partir de un botón de envío.

Dentro de estas dos cajas de texto se puede inyectar código dentro de nuestras aplicaciones web.

Es necesario que nosotros utilicemos componentes, librerías o cualquier uso para hacer un saneamiento de las entradas de datos que al final puede ser perjudicial y puede acarrear un riesgo para nuestras aplicaciones web.

**Prevención de Ataques**

**¿Qué pueden hacer los sitios individuales para protegerse de los ataques DDoS?**

Para proteger su sitio web, debe poder bloquear o absorber el tráfico malicioso. Los webmasters pueden hablar con su proveedor de alojamiento sobre la protección contra ataques DDoS. También pueden enrutar el tráfico entrante a través de un servicio de terceros de buena reputación que proporcione almacenamiento en caché distribuido para ayudar a filtrar el tráfico malicioso, lo que reduce la carga en los servidores web existentes. La mayoría de estos servicios requieren una suscripción paga, pero a menudo cuestan menos que aumentar la capacidad de su propio servidor para hacer frente a un ataque DDoS.

Google Ideas ha lanzado una nueva iniciativa, [Project Shield](http://projectshield.withgoogle.com/) , para utilizar la infraestructura de Google para apoyar la libre expresión en línea ayudando a sitios independientes a mitigar el tráfico de ataques DDoS.

## ¿Qué pueden hacer los proveedores de alojamiento, los ISP y las grandes organizaciones para proteger sus redes?

Existen muchos productos y servicios para proteger las redes grandes de los ataques DDoS y evitar que los recursos de la red se utilicen para amplificar los ataques. Arbor Networks, que proporciona datos para esta visualización, también ofrece una serie de servicios de mitigación de DDoS. Para obtener más información, visite [arbornetworks.com/research/what-is-ddos](https://www.arbornetworks.com/research/what-is-ddos).

## ¿Existen mejores prácticas a nivel de Internet que puedan mitigar el impacto de los ataques DDoS?

Mediante la colaboración continua de las numerosas partes interesadas en la mejora de Internet, una serie de esfuerzos pueden ayudar a reducir la amenaza de ataques DDoS.

Por ejemplo, hace diez años, el Grupo de Trabajo de Redes del Grupo de Trabajo de Ingeniería de Internet publicó [la BCP 38](http://tools.ietf.org/html/bcp38) (también conocida como RFC 2827) como una guía de mejores prácticas para que los ISP y los proveedores de alojamiento puedan filtrar direcciones IP falsas para reducir el impacto de la actividad DDoS sobre ellos mismos y los demás. Lamentablemente, muchos ISP aún no han implementado estas mejores prácticas, lo que impide que la comunidad de Internet en general aproveche plenamente sus beneficios.