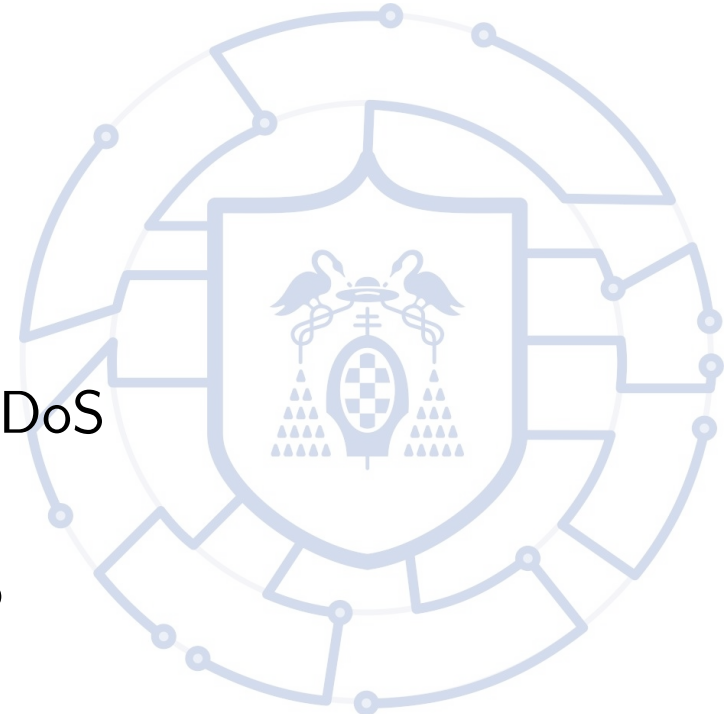
Malware para realizar ataques distribuidos

Kevin van Liebergen
Francisco Ramos
Luis Román
Miguel Ortiz

Equipo 5

Universidad de Alcalá

Índice



Introducción

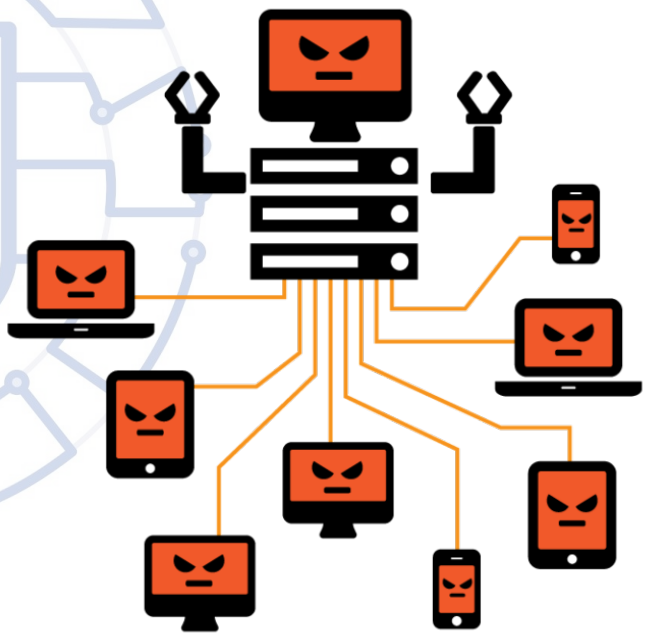
Los ataques distribuidos son malware que pueden dejar inoperativo uno o varios servicios de red, robo o minería de Bitcoins entre otros.

- Botnets
- Tipos de ataques DDoS
- Prueba de concepto
- Mitigaciones

¿Ques es una botnet?

Un Bot es un programa autónomo que realiza tareas automáticamente sin que lo sepa un usuario real.

- Robo de identidad
- Correos Spam
- Fraudes mediante click
- Ataques DDoS
- Contextos militares y políticos



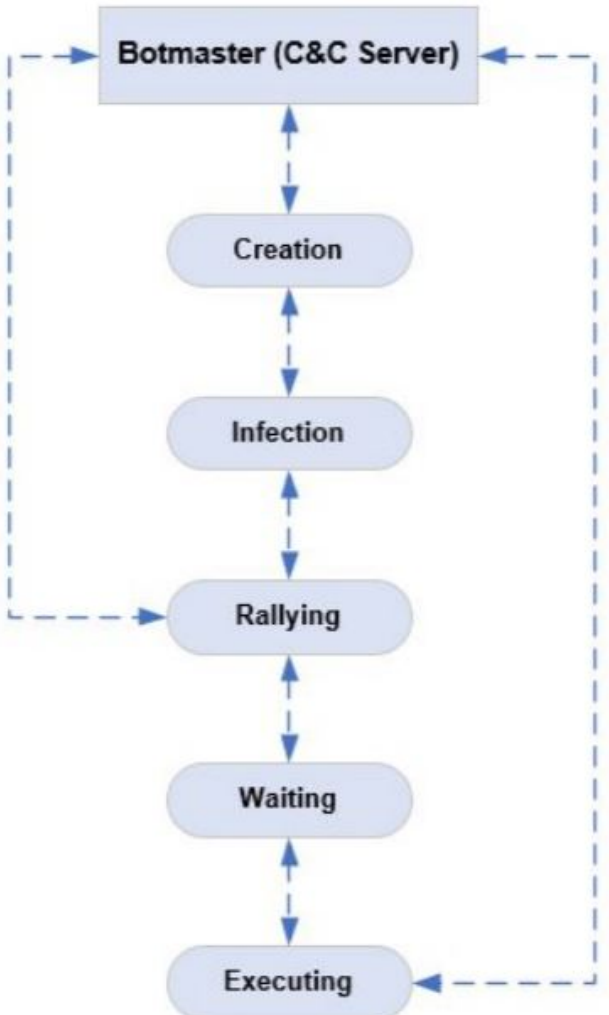
¿Cómo funciona una botnet?

En el contexto de DDoS hay dos categorías de botnet.

- Botnet estacionario.
- Botnet móvil.

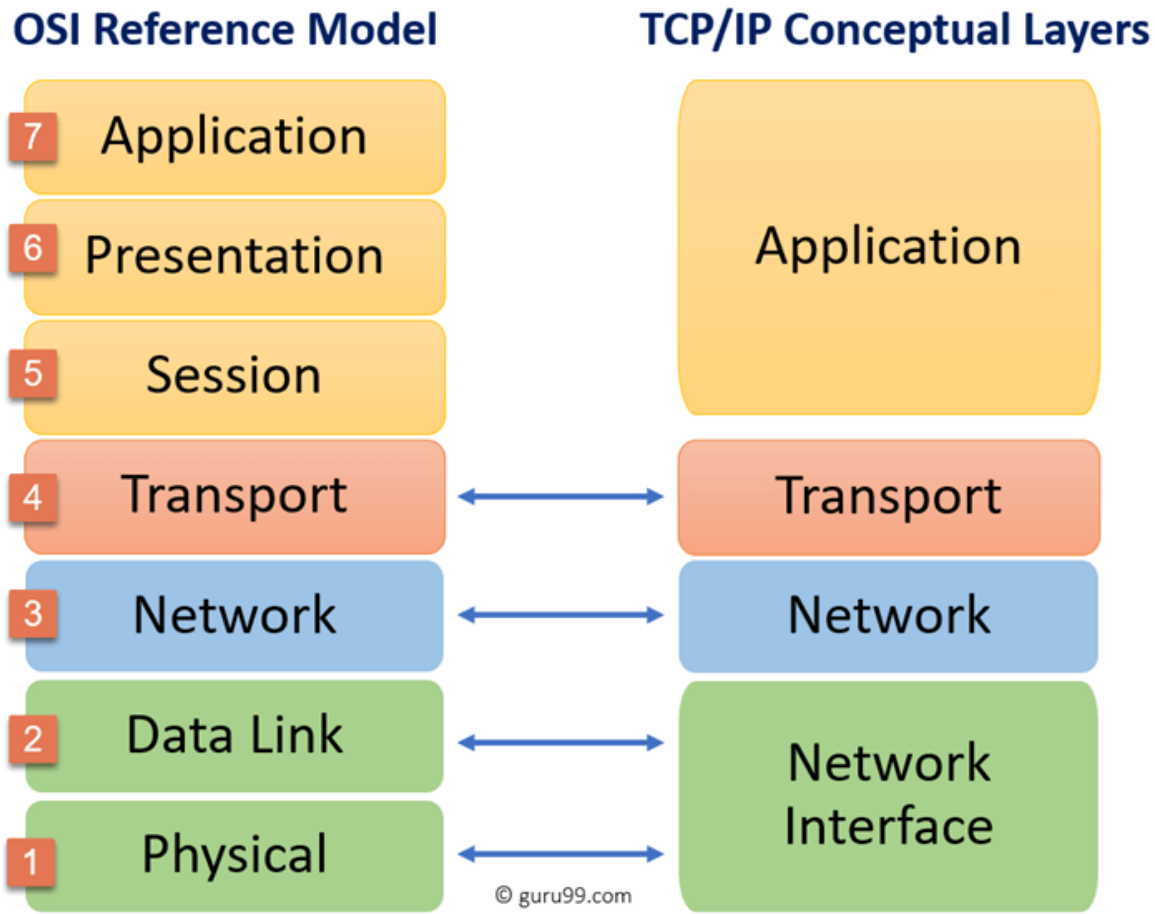
Razones de uso.

- Potentes ataques de inundación.
- Dificultad de identificar al atacante.
- Evasión de seguridad.
- No es facil de detectar en tiempo real.



Capas de red

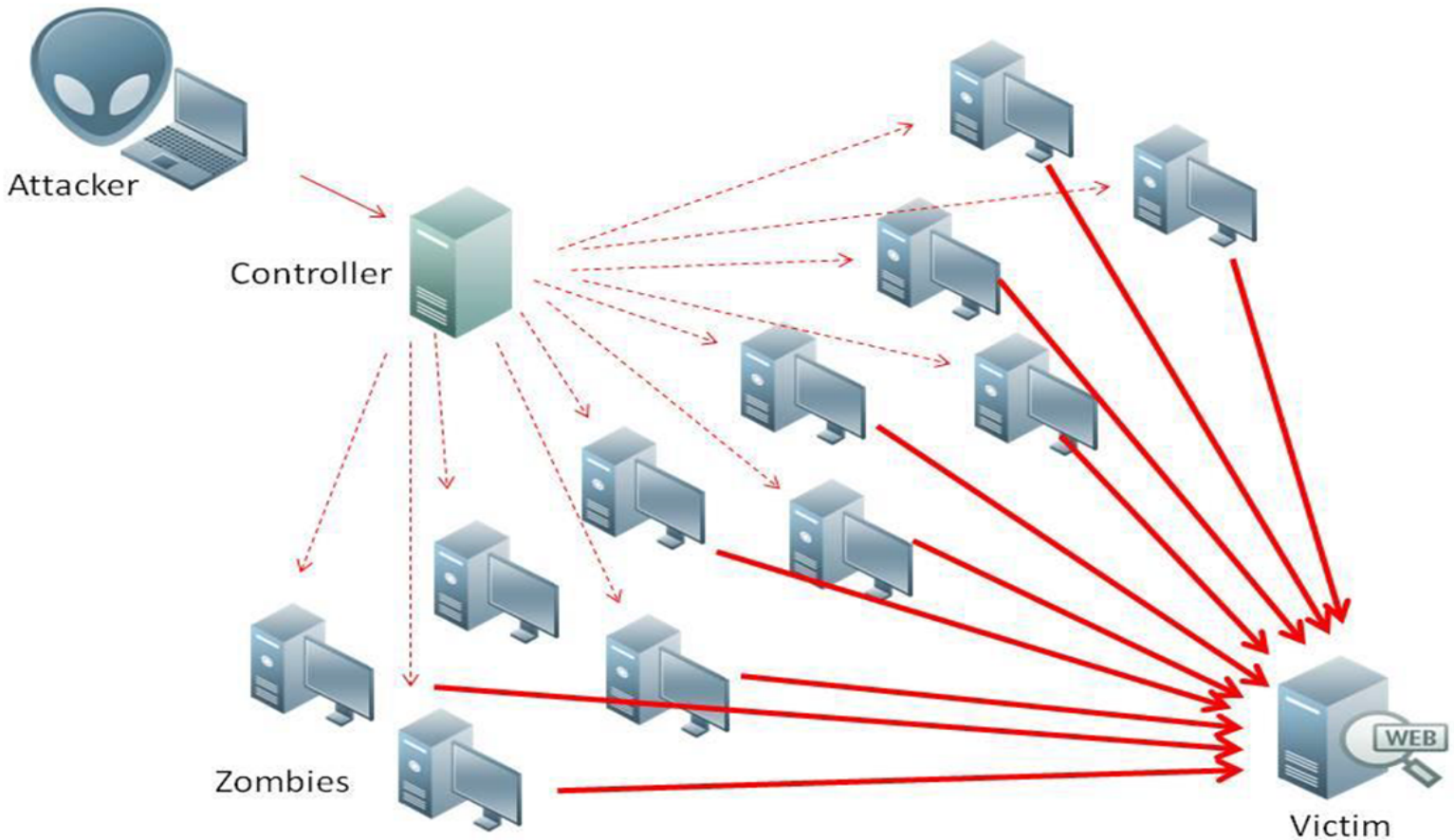
- Aplicación
- Transporte
- Red



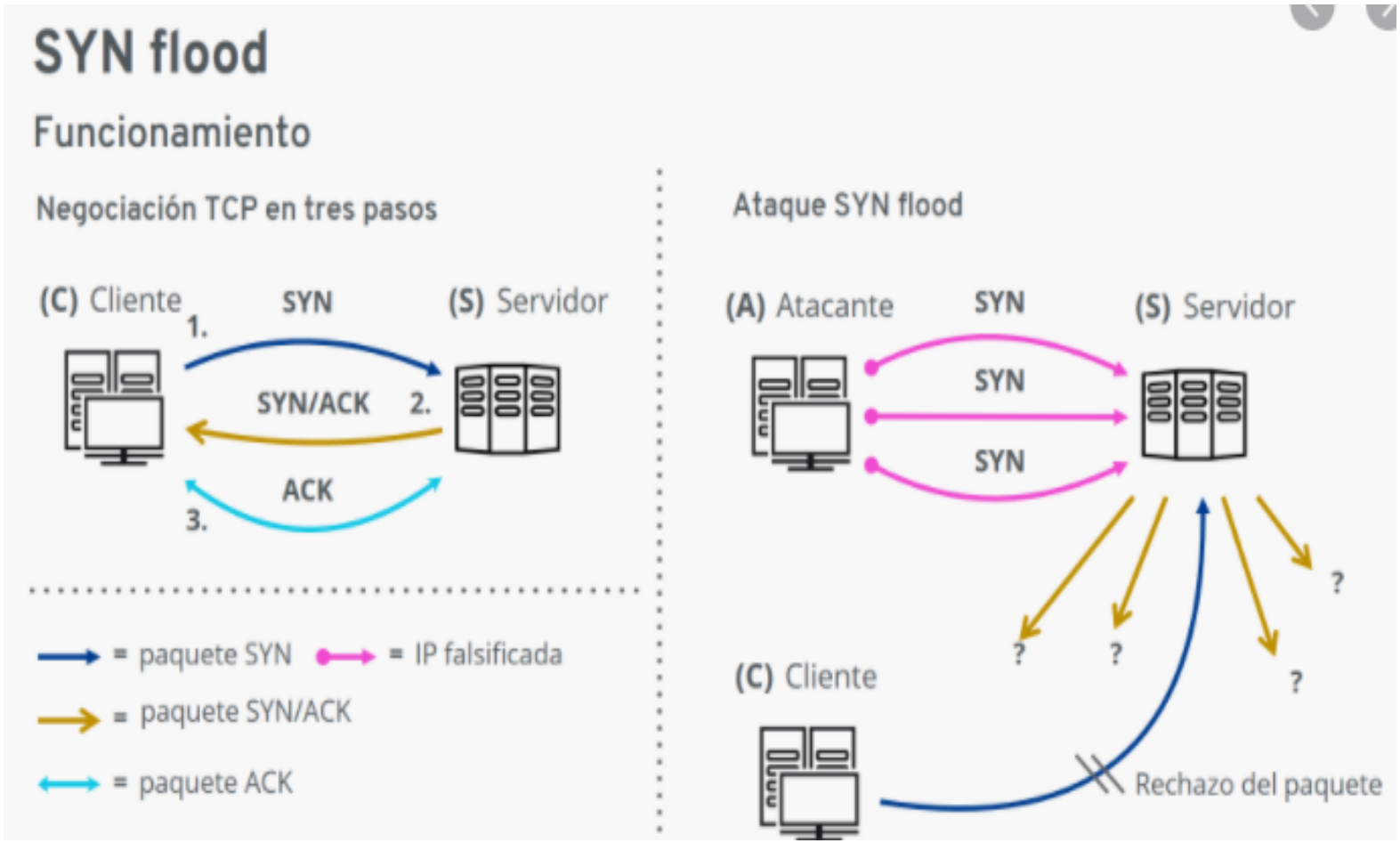
Tipos

- Aplicación
  - Smurf
  - Slowloris
  - HTTP Flood
- Transporte
  - Syn Flood
  - UDP Flood
- Red
  - ICMP Flood
  - Ping of Death
- Zero Days!

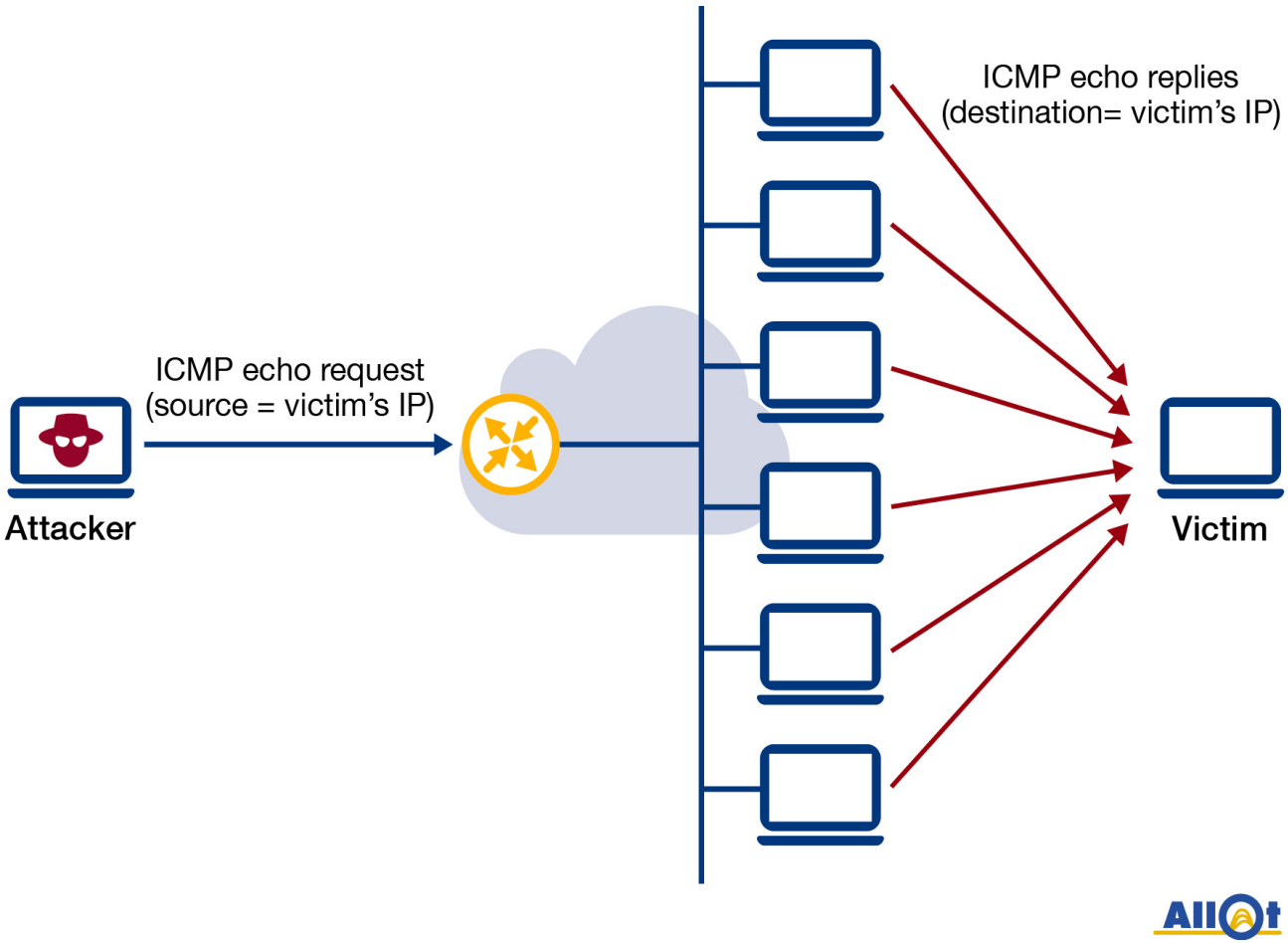
DDoS Capa Aplicación



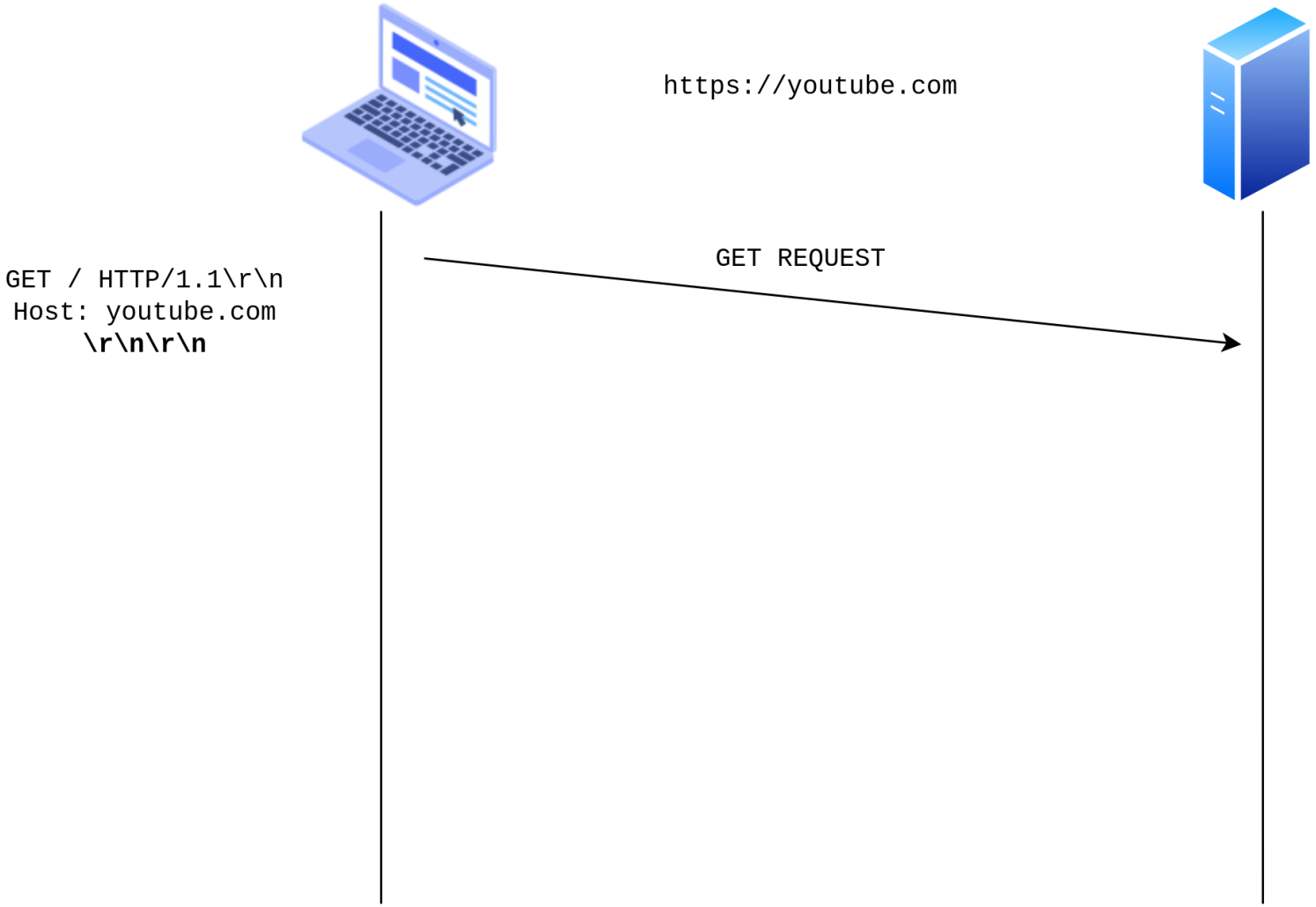
DDoS Capa Transporte



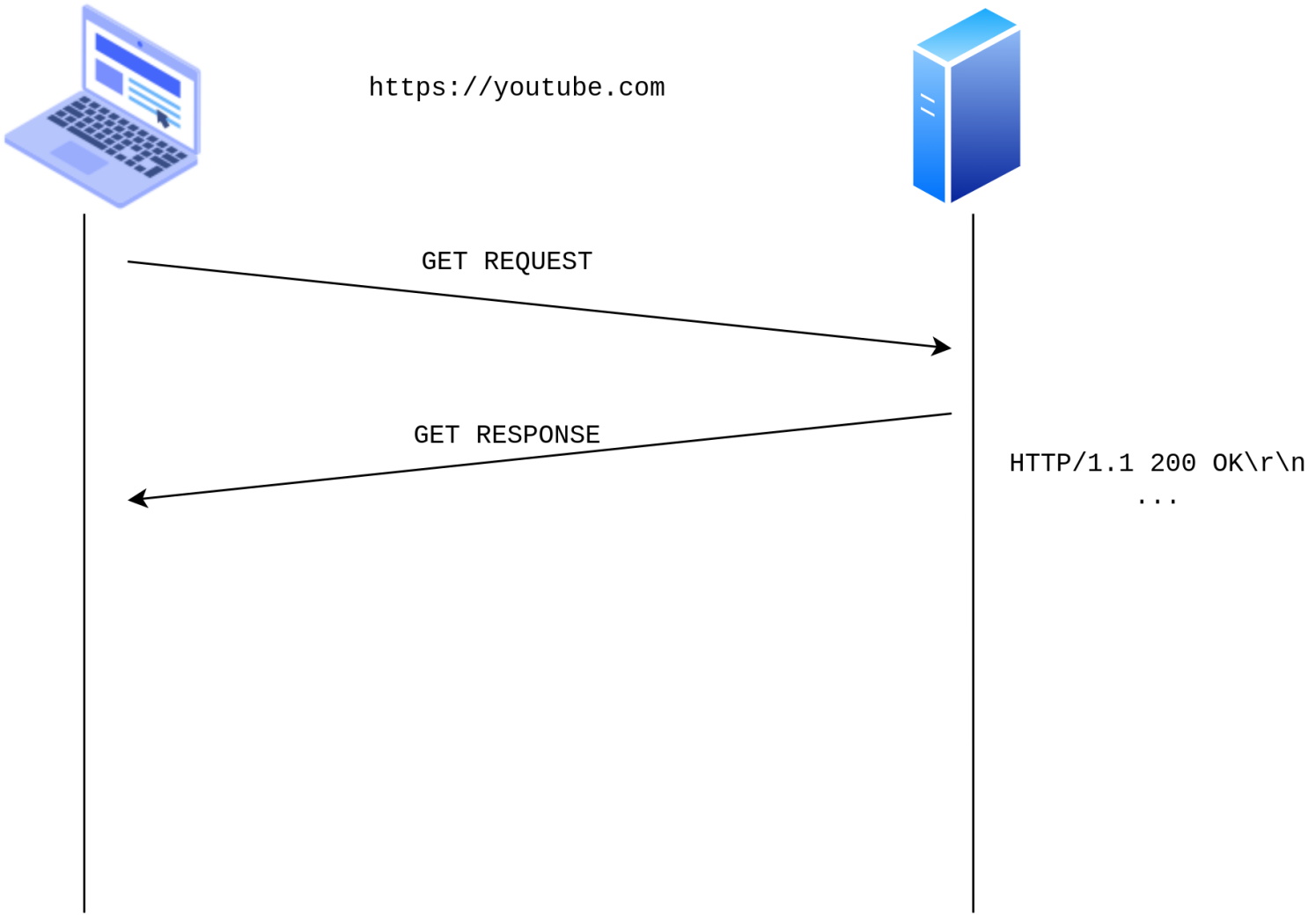
DDoS Capa Red



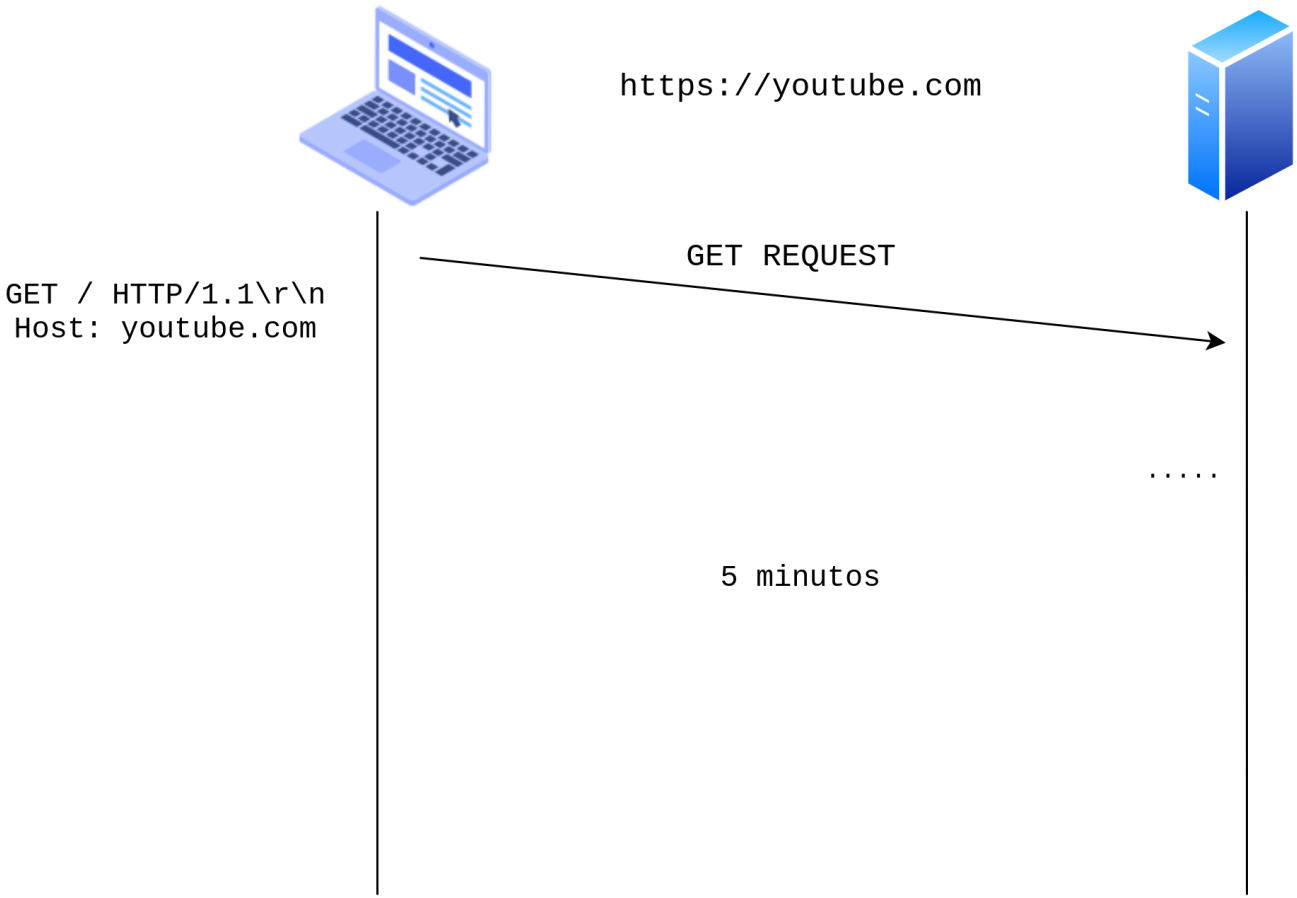
Funcionamiento Apache



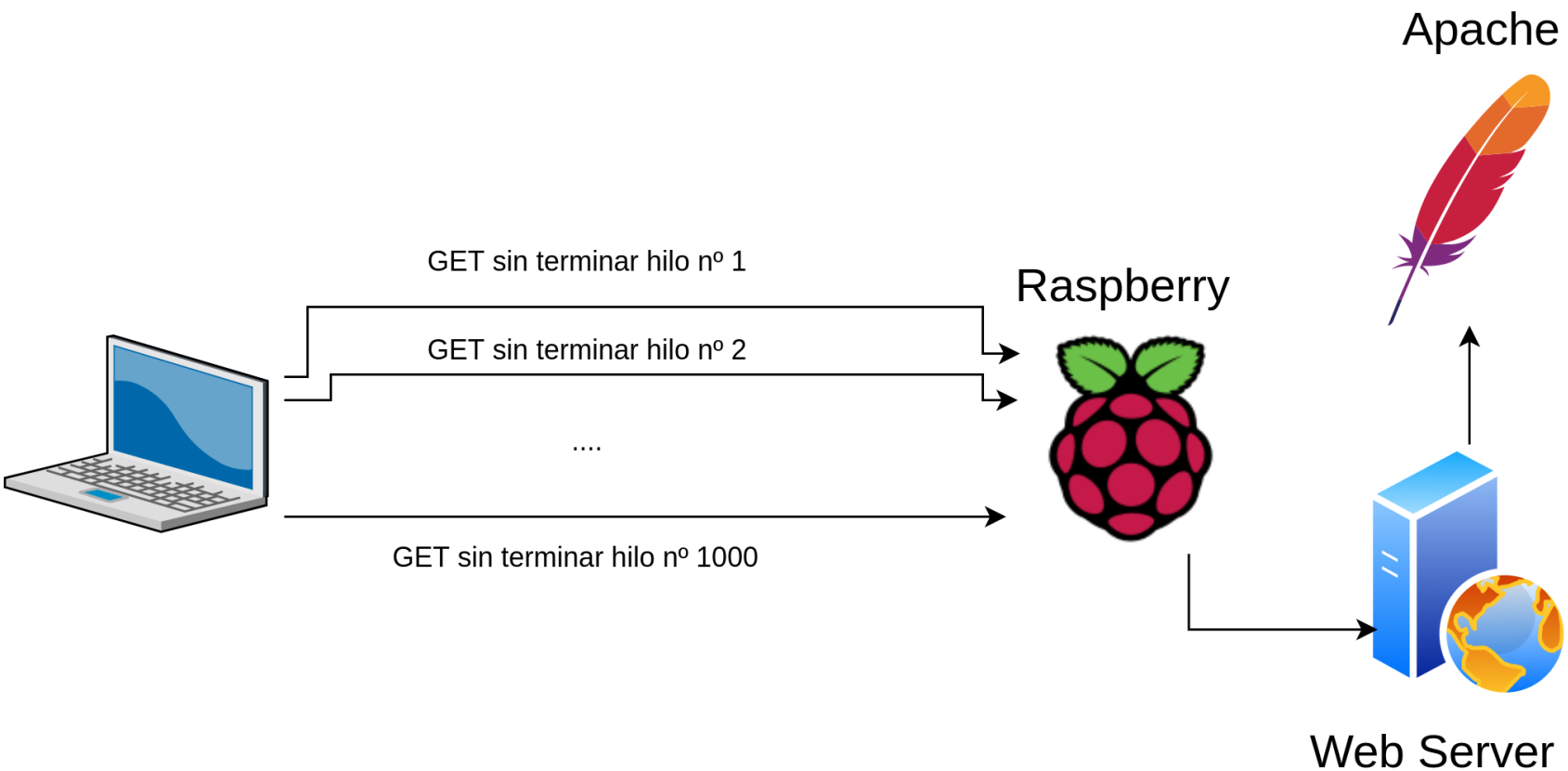
Funcionamiento Apache



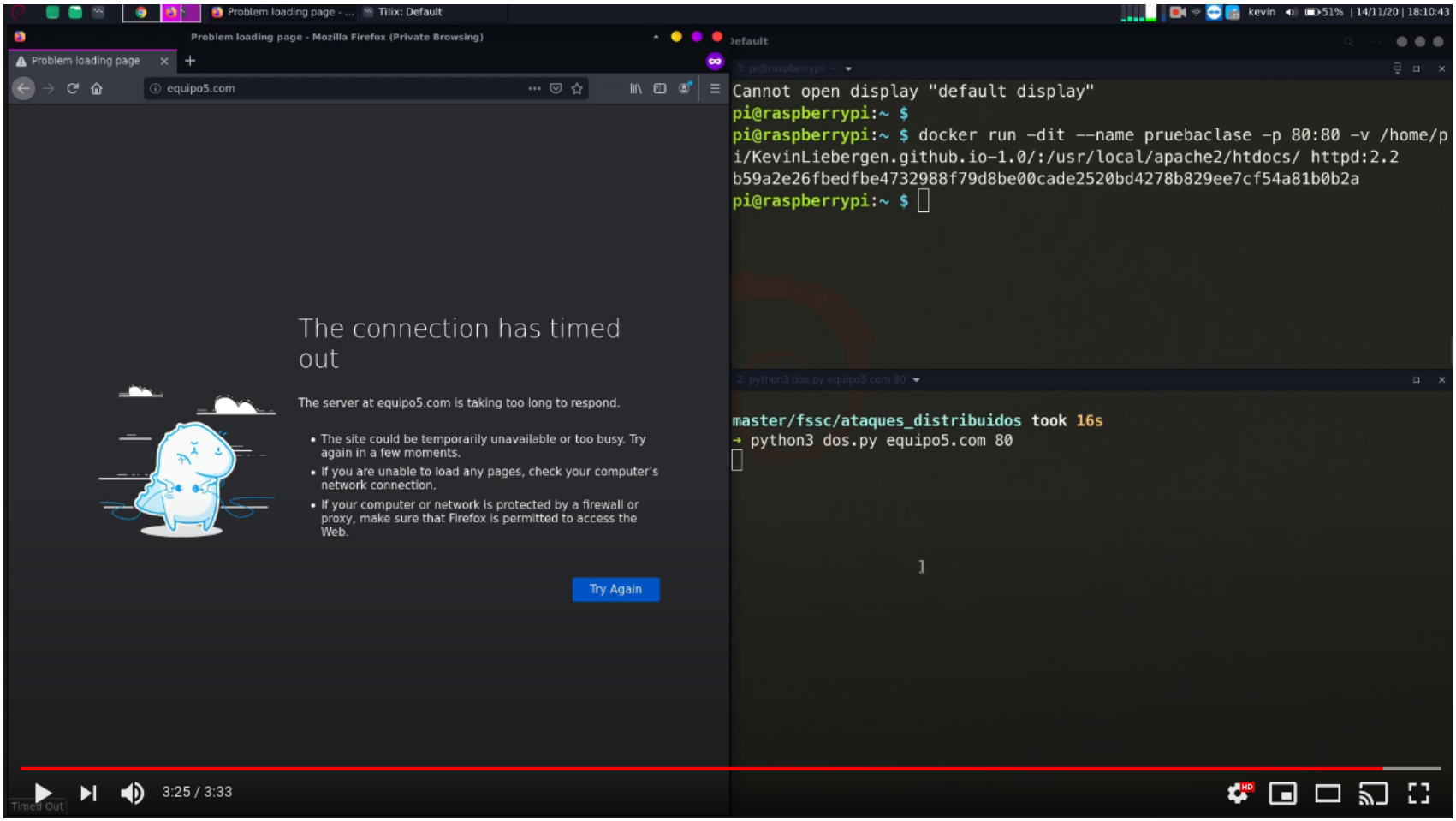
Funcionamiento Apache



Escenario de la prueba de concepto

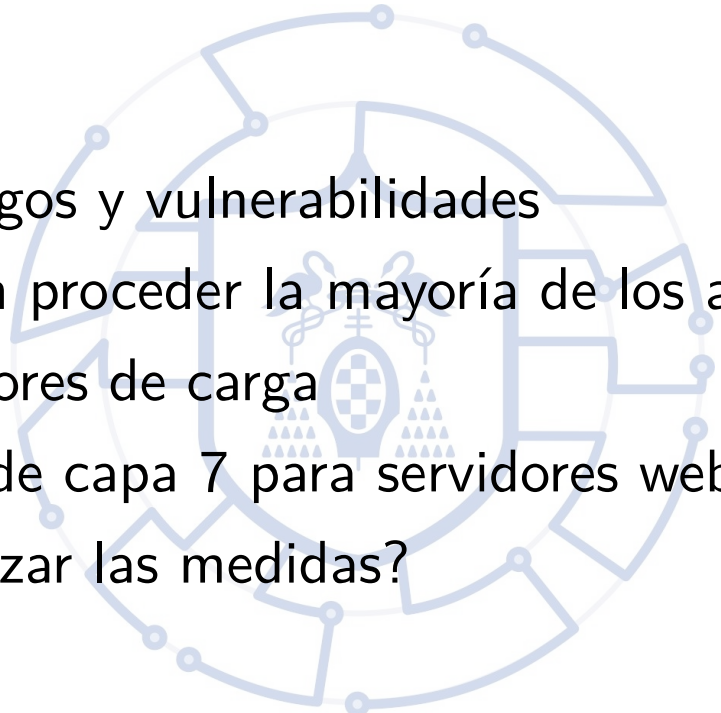


Vídeo prueba de concepto



Vídeo demo

Medidas de prevención y mitigaciones



- Evaluación de riesgos y vulnerabilidades
- ¿De dónde pueden proceder la mayoría de los ataques?
- Utilizar balanceadores de carga
- Emplear firewalls de capa 7 para servidores web
- ¿Dónde debo realizar las medidas?

Medidas en los equipos de red perimetrales

- Control sobre las IPs
  - Limitar el número de conexiones por dirección IP
  - Bloquear IPs de países con los que no nos comuniquemos
  - Activar protecciones frente a ataques SYN Flood
  - Limitar el número de peticiones por segundo desde una misma dirección IP
  - Utilizar Dynamic IP Restrictions (DIR)

Medidas en los equipos de red perimetrales

- Control sobre HTTP
  - No permitir conexiones HTTP lentas (cerrarlas)
  - Bloquear peticiones HTTP cuyo User-Agent no sea estándar
  - Implementar sistemas de caché para devolver peticiones sin tener que ser procesadas por el backend
  - Implementar sistemas captcha en formularios públicos
- Firewall de aplicaciones para el servidor de aplicaciones
- Activar 'mod-dosevasive' en apache destinado contra DDoS

Medidas en los equipos de red intermedios

Para los ataques que puedan proceder desde dentro o los que consigan atravesar las medidas anteriores:

- Emplear técnicas de filtrado de rutas
- Verificar la dirección de origen en los paquetes que se reenvian
- Utilizar soluciones que proporcionen dispersión geográfica
- Ajustar límites de conexión y tiempos de espera
- Aplicar listas de control de acceso

Medidas para ataques de mayor intensidad

Pueden no ser suficientes las medidas anteriores

- Comprar servidores que absorban tráfico y peticiones
- Soluciones anti-DDoS hardware
- Utilizar servicios en la nube

Existen infidad de sistemas anti-DDoS, destacan:

Medidas para ataques de mayor intensidad

Solución	Localización	Tipo de protección	Capacidades frente a taques
Imperva DDoS Protection[1]	Cloud CDN	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Hasta 6 Tbps y 65 billones de pps.
Kona Site Defender de Akamai[2]	Cloud CDN	Protección en capa de aplicación (DNS requiere de FastDNS) e infraestructuras (de capa 3 a 7).	Hasta 61 Tbps
Cloudflare DDoS Protection[3]	Cloud	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Hasta 30 Tbps
Microsoft Azure DDoS Protection[4]	Cloud	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Varios gigabytes
Radware DDoS Protection[5]	Hibrido	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	Hasta 300Gbps y 230 millones de pps.
AWS Shield Advanced[6]	Cloud	Protección en capa de aplicación e infraestructuras (de capa 3 a 7)	
Neustar[7][8][9]	Cloud, Hibrido	Protección en capa de aplicación e	Hasta 6 Tbps

¡Gracias!

¿Preguntas?