
10. Denegación de Servicio
Julio Javier Iglesias Pérez
C|EH
Julio Iglesias Pérez

Denial of Service (DoS)

Un ataque DoS es un ataque en un equipo o una red previniendo el uso legítimo de sus recursos.

En este tipo de ataque el atacante inunda al sistema de la víctima con solicitudes al servicio o tráfico no legítimo.

Distributed Denial of Service (DDoS)

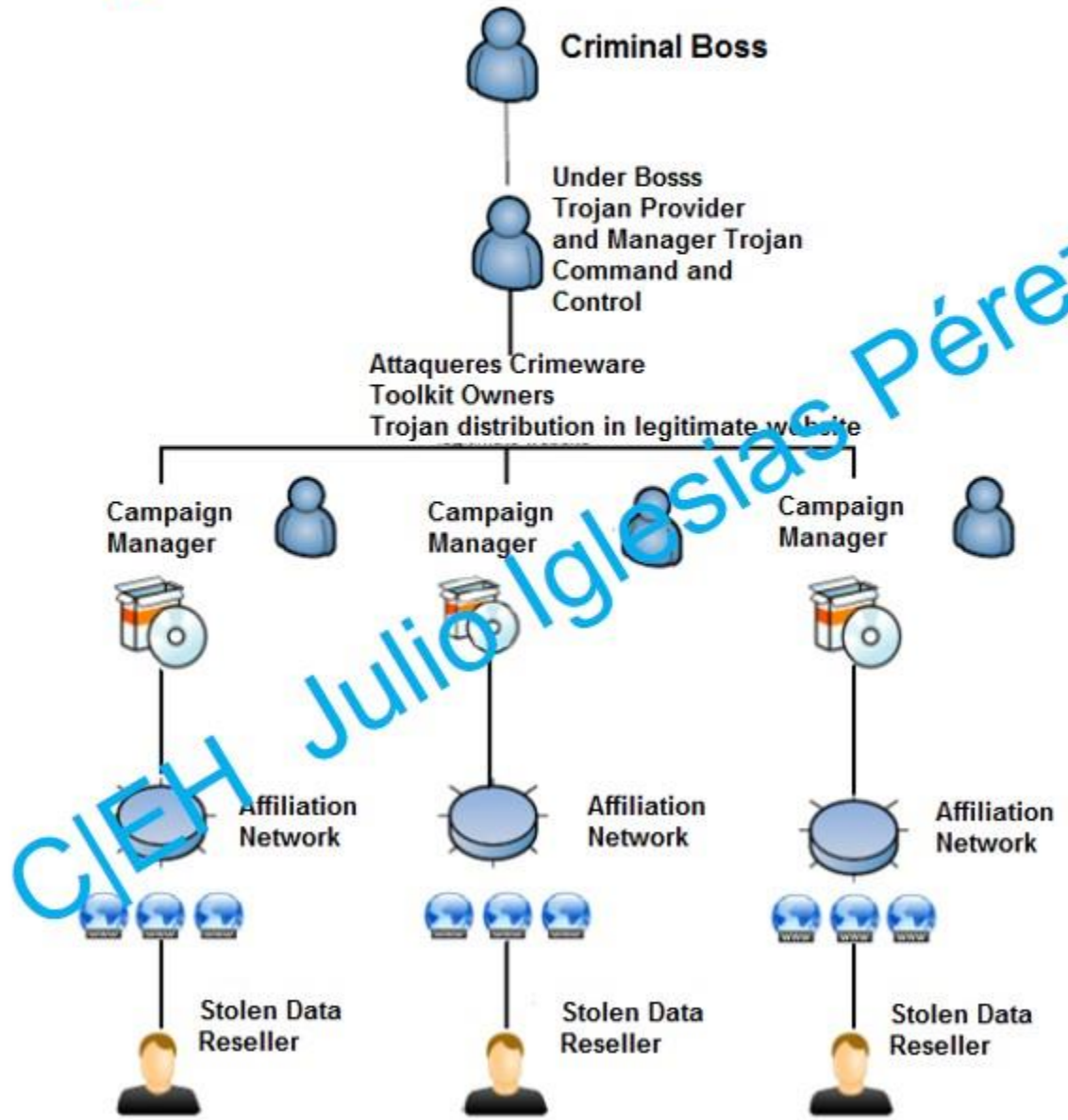
Los ataques DDoS son ataques distribuidos, muchos atacantes.

Utilizando equipos comprometidos (zombis).

Síntomas de un ataque DoS

- Usualmente rendimiento lento de la red.
- No disponibilidad de un sitio web particular.
- Inhabilidad de acceder a un sitio web.
- Incremento dramático de correos spam recibidos.

Organigrama de un Ciberataque



Técnicas de ataque DoS

- Bandwidth Attacks: Consumir el ancho de banda envíando muchísimos paquetes.
- Service request floods: Un atacante o grupo de atacantes zombis intenta agotar los recursos de la red. Muchas conexiones válidas desde una fuente válida.
- SYN Attack: El atacante envía solicitudes TCP SYN falsas a la víctima. El blanco entonces envía un SYN ACK en respuesta. El blanco no recibe ninguna respuesta ya que la dirección fuente es falsa.

Técnicas de ataque DoS

- SYN Flooding: Su ventaja es que muchos hosts implementan el three-way handshake. Cuando el host B recibe una solicitud SYN desde A, debe permanecer siguiendo a la conexión parcialmente abierta en una "listen queue" por al menos 75 segundos. La cuestión es que el atacante envía múltiples SYN requests pero nunca responde al SYN/ACK. La habilidad de remover el host de la red por 75 segundos puede ser utilizada como un ataque DoS.
- ICMP Flood Attack: Ataques con una fuente falsa. Echo requests, echo replies.

Técnicas de ataque DoS

- Peer-to-peer Attacks: Utilizando estos ataques, los atacantes pueden instruir a los clientes a compartir sus hubs punto a punto para desconectarse de su red y conectarse al sitio web falso de la víctima. Explotan fallas encontradas en la red DC++. Utilizando este método los atacantes pueden realizar ataques masívos DoS y comprometer sitios web.

Técnicas de ataque DoS

- Ataques DoS permanentes: Conocidos como phlashing, son ataques que causan daños irreversibles al hardware del sistema. Estos sabotean el hardware del sistema, requiriendo a que la víctima los remplace. Este ataque es realizado por un método denominado "bricking a system", envíando actualizaciones de hardware fraudulentas a las víctimas.
- Application Level Flood Attacks: Inundan el ancho de banda con aplicaciones específicas, pérdida de servicio de mails, recursos de red, etc.

Botnet

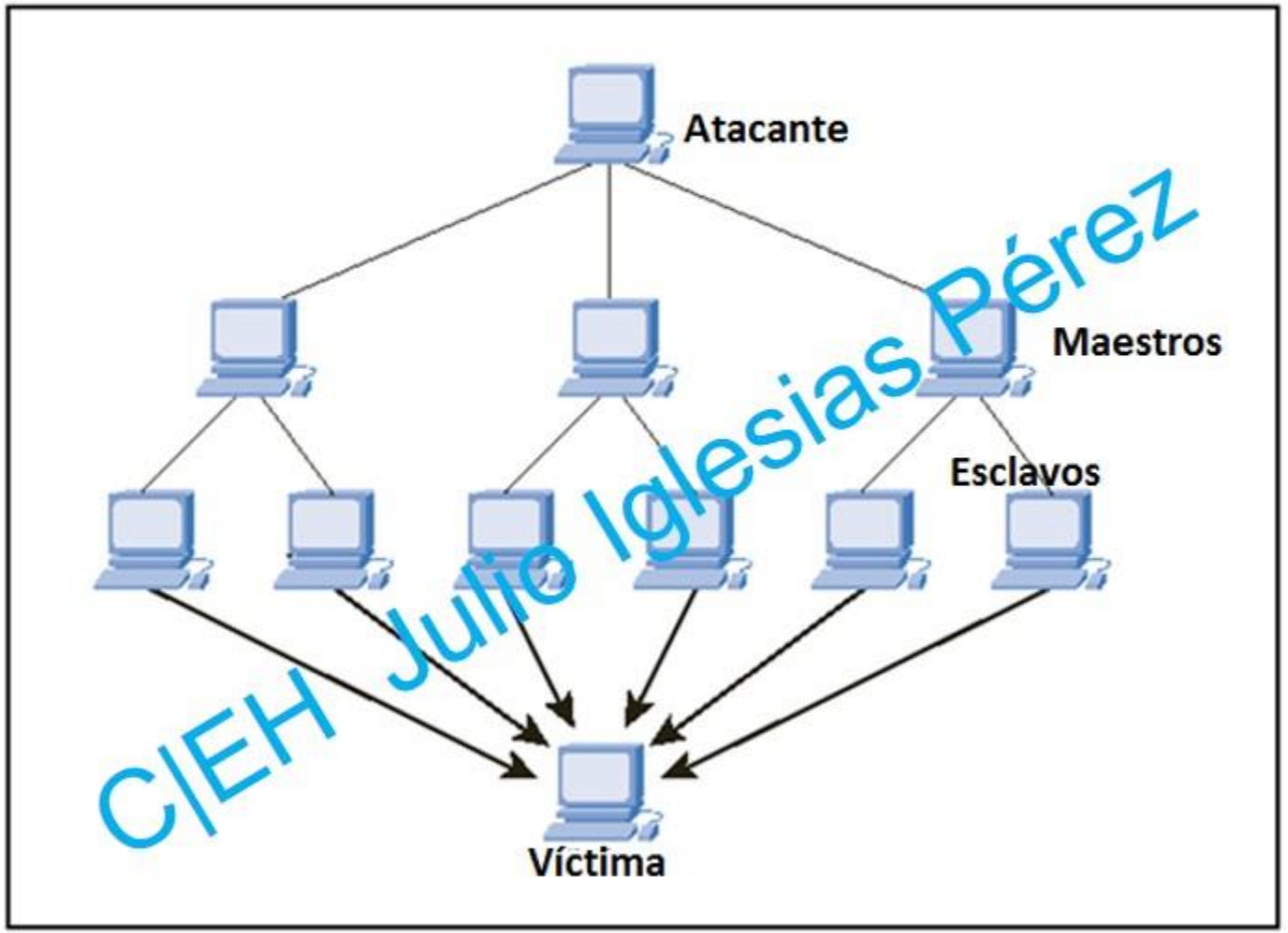
Son aplicaciones de software que corren automáticamente realizando tareas automatizadas por el Internet.

Troyano Botnet: Shark

Poison Ivy: Botnet Command Control Center

Troyano Botbet: Plugbot

Ataque DDoS



Herramienta LOIC

Low Orbit Ion Cannon. Con esta herramienta botnet voluntaria lograron bajar a Visa y Mastercard. Con unos pocos equipos (800) lograron bajar visa y con otros pocos (1000) a Visa, 10 Gb por segundo.

Herramientas DoS

Un atacante, una víctima

DoSHTTPS 2.5.1, Sprut, PHP DoS

Contramedidas

Técnicas de detección: Identificar y discriminar tráfico ilegítimo e incrementar el flash de eventos desde tráfico legítimo. Si vemos que tenemos un botnet en nuestra red, hay que neutralizarlo. Algunas técnicas son:

- Activity Prolifing: Se utilizarán técnicas manuales o automáticas para determinar, qué es actividad normal, que es actividad anormal, línea base.

Contramedidas

- Wavelet Analysis: Describe una señal de entrada en términos de componentes espectrales, analizar la presencia de esos espectros nos indicarán o no una anomalía. Provee tiempo actual y descripción frecuente. Determinan el tiempo que ciertos componentes de frecuencia están presentes.

Contramedidas

- Sequential Change-Point Detection: Algoritmos de detección de cambio de punto aíslan las estadísticas de cambio causadas por los ataques. Inicialmente filtran el los datos del tráfico del objetivo por dirección, puerto o protocolo y almacena los resultados en una serie de tiempo. Para identificar y localizar un ataque DoS, el algoritmo Cusum identifica desvíaciones en el frente actual. También puede ser utilizado para identificar las actividades de escaneo típicas de los worms en la red.

Estrategias y contramedidas DoS/DDoS

1. Absorber el ataque: Utilizar capacidad adicional para absorber el ataque, requiere pre planeación, y recursos adicionales.
2. Degradando servicios: Identificar servicios críticos y detener los servicios no críticos.
3. Apagando los servicios: Apagar todos los servicios hasta que el ataque haya disminuido.

Contramedidas para ataque DDoS

- Desviar los ataques
- Mitigar los ataques
- Análisis forense post-ataque
- Prevenir posibles ataques
- Neutralizar controladores
- Proteger a las víctimas secundarias

Protegiendo a las víctimas secundarias

- Concientizar de los problemas de seguridad.
- Instalar A.V. y anti-troyanos.
- Construir mecanismos de defensa.
- Deshabilitar servicios innecesarios.

Neutralizar controladores

- Analizar el tráfico de red.
- Neutralizar los controladores de Botnets.
- Direcciones falsas.

Prevenir posibles ataques

- Filtros de entrada.
- Filtros de salida.
- Intercepción TCP.

Desviar los ataques

- Los sistemas que están configurados con seguridad limitada, también conocidos por Honeypots, actúan como un seductor para un atacante.
- Servir como un medio para obtener información acerca de los atacantes almacenando un registro de sus actividades y aprender qué tipos de ataques y herramientas de software utilizan los atacantes.
- Utilizar un enfoque de defensa en profundidad con IPSec en distintos puntos de red para desvíar el tráfico sospechoso DoS a varios Honeypots.

Mitigar los ataques

Load Balancing

1. Los proveedores pueden incrementar el ancho de banda en conexiones críticas para prevenir que se vayan abajo en el evento de un ataque.
2. Servidores de replicación puede proveer protección adicional failsafe.
3. Balancear la carga a cada servidor en una arquitectura de múltiples servidores puede mejorar ambos rendimientos normales como también mitigar los efectos de un ataque DoS.

Throttlling

1. Este método establece routers que accedern a los servicios con lógica para ajustar (throttle) el tráfico de ingreso a los niveles que van a ser seguros para el servidor para procesar.
2. Este proceso puede prevenir flood damage a los servidores.
3. Este proceso puede ser extendido para acelerar el tráfico de un ataque DoS versos el tráfico de usuarios legítimos para mejores resultados.

Análisis forense post-ataque

Analizar el router, firewall, los logs IDS para identificar la fuente del tráfico DoS. Aunque los atacantes generalmente spoofean su dirección verdadera, se seguirá la pista con la ayuda de los ISPs y agencias de leyes. Un análisis de patrón de tráfico puede ser analizado para buscar carácterísticas específicas dentro del tráfico del ataque.

Técnicas para defenderse contra Botnets

- RFC 3704: Los paquetes deben ser de una fuente válida, alojados en una asignación de direcciones, consistente con la topología y asignación de espacio. Cualquier tráfico que venga de direcciones IP reservadas o sin uso es falso y debería ser filtrado en el ISP antes de que entre al vínculo de Internet.
- Black Hole Filtering: Son puestos en la red donde el tráfico es renviado y dropped. La técnica RTBH utiliza actualizaciones del protocolo de enrutamiento para manipular las tablas en el borde de la red para dropear el tráfico no deseado antes de que entre el proveedor de servicio de red.

Técnicas para defenderse contra Botnets

- Cisco IPS Source IP Reputation Filtering: Cisco IPS recibe actualizaciones de amenazas desde el SensorBase Network de Cisco, que contiene información detallada acerca de las amenazas conocidas en Internet, incluyendo ataques en serie, cosechadoras de Botnets, brotes de Malware, y redes oscuras.
- DDoS Prevention Offerings from ISP or DDoS Service: Encendiendo el IP Source Guard en los switches de la red previene a un host enviar paquetes falsosy volverse un bot.

Contramedidas DoS DDoS

- Mecanismos de encriptación eficientes necesitan ser propuestos para cada tecnología.
- Mejores protocolos de enrutamiento son deseables, particularmente para multi-hop WMN.
- Deshabilitar servicios inseguros y no deseados.
- Bloquear todos los paquetes originados desde los puertos de servicio que bloquean el tráfico de servidores reflectores.
- Actualizar el kernel a la última versión.
- Prevenir la transmisión fraudulenta de paquetes en el nivel ISP.
- Implementar radios cognitivas en la capa física para manejar el bloqueo y el tipo codificación de los ataques.

Contramedidas

1. Configurar el firewall para denegar Internet Control Message Protocol (ICMP) externo.
2. Prevenir el uso de funciones innecesarias como gets, strcpy, etc.
3. Asegurar la administración remota y prueba de conectividad.
4. Prevenir que las direcciones de retorno sean sobrescritas.

Contramedidas

5. Los datos procesados por un atacante deben ser detenidos de ejecución.
6. Realizar validación de entradas.
7. La tarjeta de red es una puerta de enlace de los paquetes. Utilizar una mejor tarjeta de red para manejar números largos de paquetes.

Protección DoS/DDoS a livel ISP

- La mayoría de los ISP simplemente bloquean todas las solicitudes durante un ataque DDoS, denegando tráfico legítimo.
- Los ISP ofrecen protección DoS in-the-cloud para los vínculos de Internet así ellos no se saturan por el tráfico.
- El tráfico de ataque es redirigido al ISP durante el ataque para que sea filtrado y enviado de vuelta.
- Los administradores puede solicitar a los ISP que bloqueen la IP original afectada y muevan su sitio a otra IP luego de realizar una propagación DNS.

Habilitando TCP Intercept en IOS de Cisco

1. Definir una lista de IP extendido: access-list access-list-number {deny | permit} tcp any destination destination-wildcard
2. Habilitar TCP Intercept: ip tcp Intercept list access-list-number

TCP Internep puede operar en modo activo y pasívo (watch mode). Por defecto está en intercept mode.

El comando para configurar TCP Intercept en modo configuración global es: ip tcp intercept mode {intercept | watch}.

Protección DDoS avanzada

IntelliGuard DDoS Protection System (DPS)

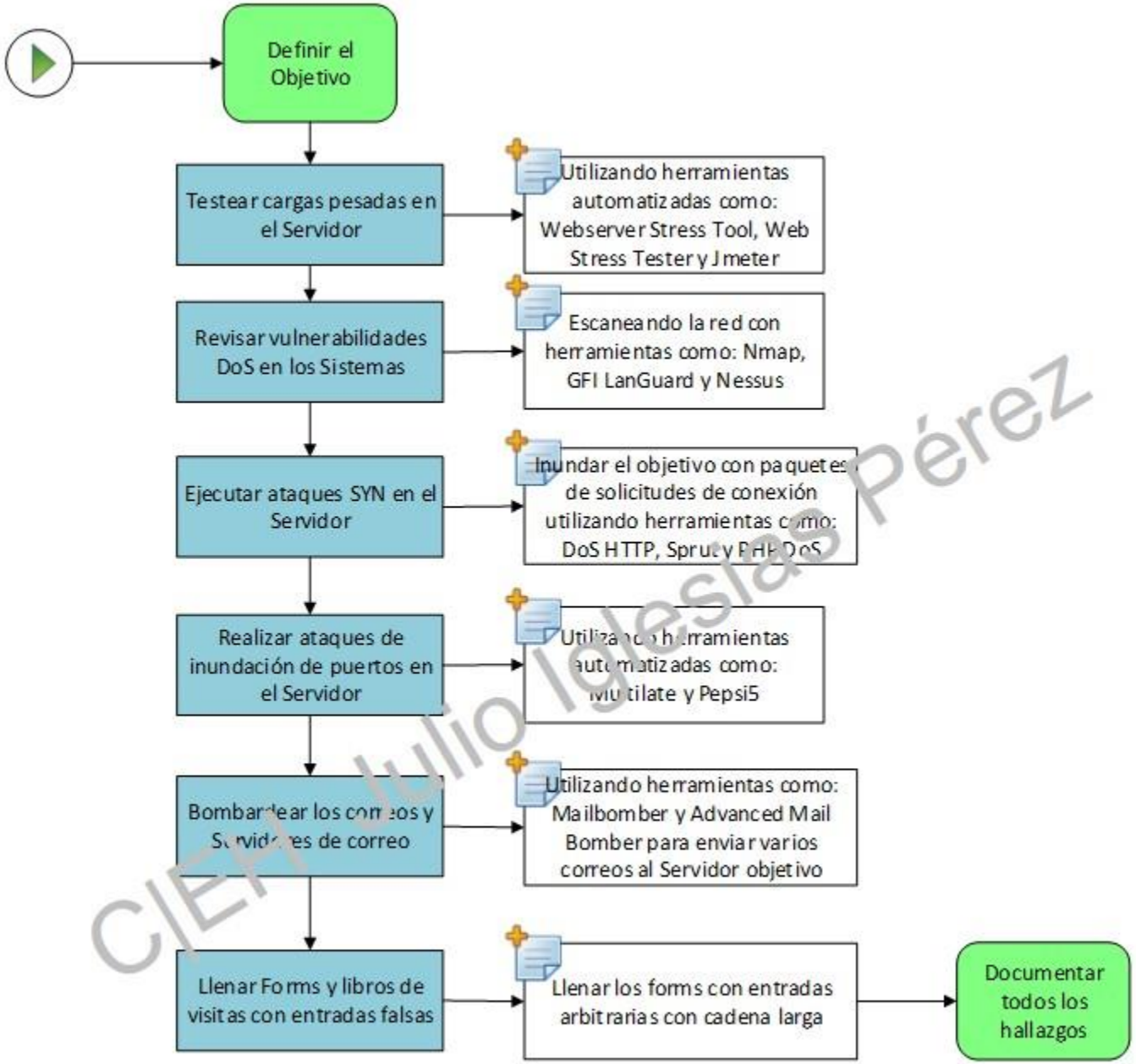
Ayuda a mitigar los ataques DDoS utilizando un diseño que se enfoca en pasar tráfico legítimo que descargar tráfico de ataque. Su Learn-Rank-Protect-Strategy identifica sitios accedidos por clientes y prioriza continuamente y ranquea su acceso. Su multi-level-traffic-managemente configura límites de tráfico y garantiza la administración del tráfico para cada parte de la red.

Protección DDoS

- Herramientas de protección DoS/DDoS: Netflow analyzer, etc.

Test de intrusión DoS

- Debe ser incorporado en un test de intrusión para investigar si la red es susceptible a este tipo de ataques.
- Una red vulnerable no puede manejar una gran cantidad de tráfico.
- DoS Pen Testing determina mínimo de umbrales para los ataques DoS.
- El principal objetivo de un DoS Pen Testing es floodear una red objetivo con tráfico.




¡Muchas Gracias!
C|EH Julio Iglesias Perez