UNIDAD DE SERVIDORES DE SISTEMAS

MITIGACIÓN DE ATAQUES DOS/DDOS A SITIOS WEB (CAPA 7)

JUAN ANTONIO GONZÁLEZ RAMOS

JUANAN@USAL.ES

UNIDAD DE SISTEMAS, SI-CPD

UNIVERSIDAD DE SALAMANCA

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

VNiVERSiDAD D SALAMANCA
1218 - 2018

SICPD
Servicios Informáticos
CPD

UNIDAD DE SERVIDORES DE SISTEMAS

NOS ATACAN… ¿PERO POR QUÉ?

- Objetivos del ataque
  - Bloquear un sitio web
    - Motivos ideológicos, chantaje, causar daño…
  - Encubrir u ocultar otras acciones
    - Ataques a otros puntos de la infraestructura
    - Robo de datos
  - Provocar un reinicio del sistema
- Consecuencias del ataque
  - Pérdida de reputación
  - Pérdida de negocio
  - Pérdida de clientes

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

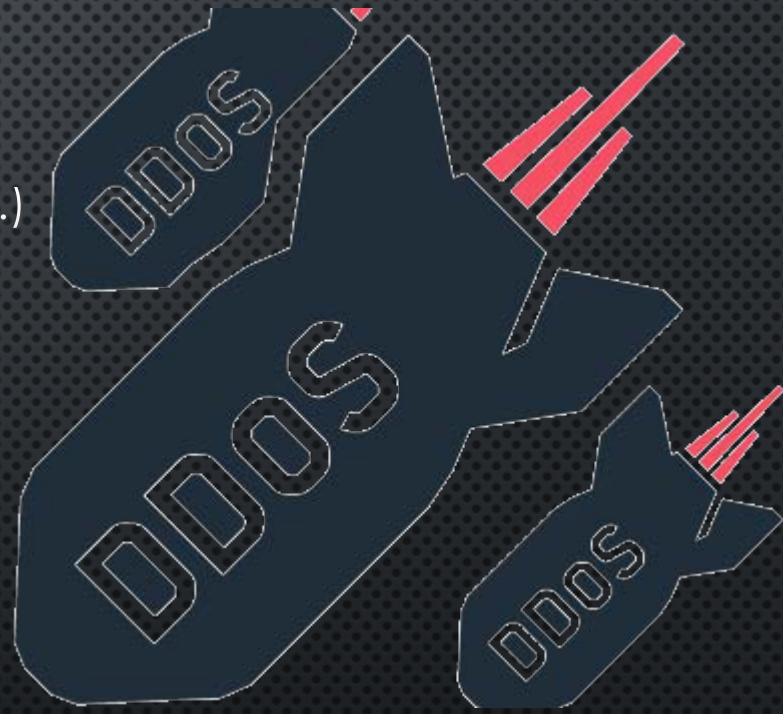
VNiVERSiDAD D SALAMANCA 1218 - 2018

SICPD Servicios Informáticos CPD

UNIDAD DE SERVIDORES DE SISTEMAS

PERO, ¿QUÉ ES UN ATAQUE DOS?

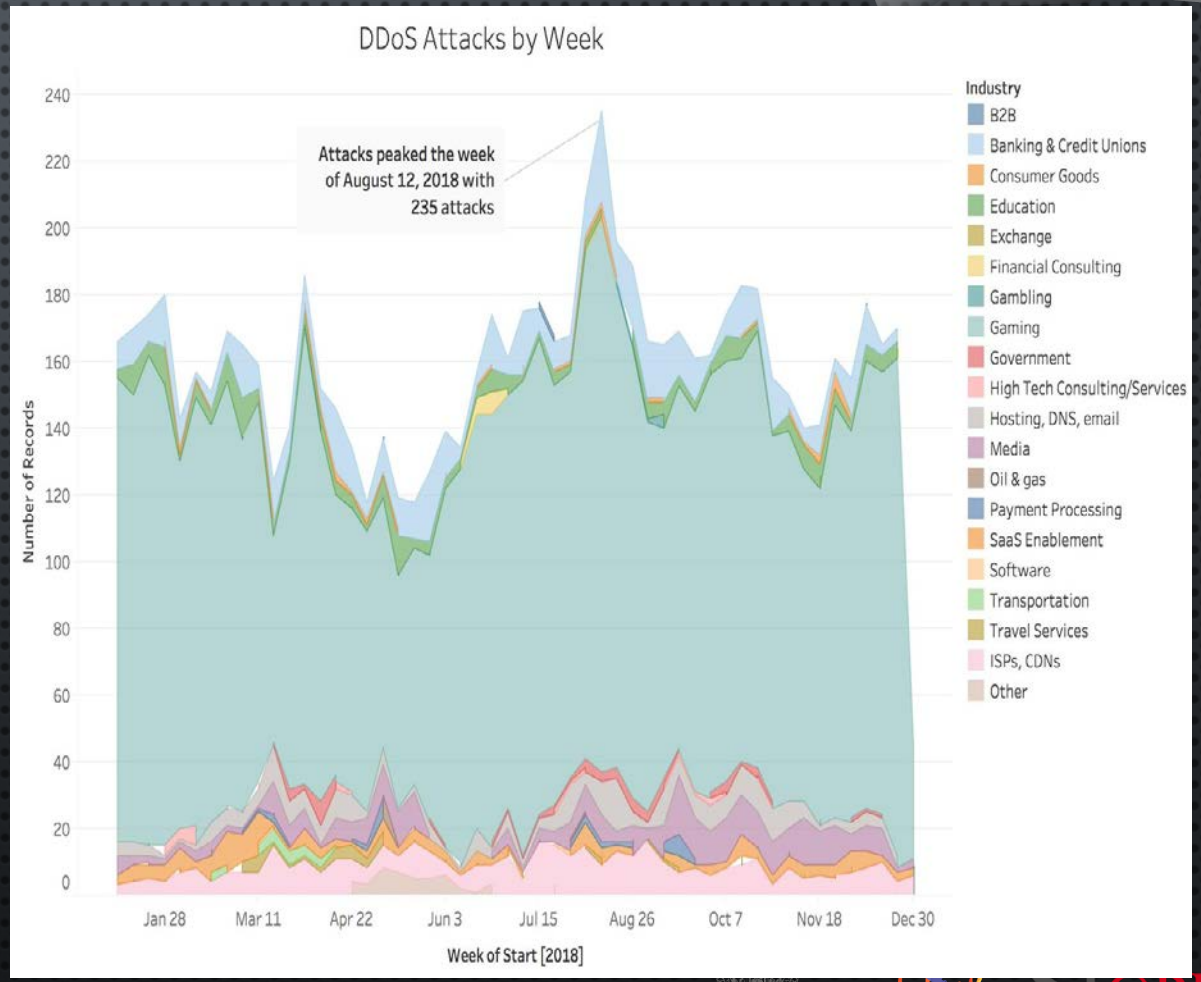
- Ataque que agota o consume todos los recursos
  - Varias formas
    - Acaparando un recurso
      - Volumétricos, por inundación (TCP SYN, inundación HTTP…)
      - Reflexivos (NTP, DNS, SNMP…)
    - Sobrecargando su uso
      - Agotamiento de recursos (CPU+memoria+disco)
  - Complicados de evitar
    - Casi siempre distribuídos
    - Muy escalables
    - Es difícil trabajar si los recursos están consumidos



UNIDAD DE SERVIDORES DE SISTEMAS

ATAQUES DDOS SEGÚN SU DESTINO DE ATAQUE.

- Ataques a la red o volumétricos
  - Objetivo de congestionar la red
  - Ataques típicos como UDP/ICMP flood
- Ataques de protocolo
  - Saturación de ciertos puertos
    - DNS, NTP…
  - Típicos el SYN flood y el TCP packet
- Ataques a aplicaciones (capa 7 del OSI)
  - Ralentización de su funcionamiento
    - Tipos LOW o SLOW
  - Consumo de recursos de servidores



UNIDAD DE SERVIDORES DE SISTEMAS

ATAQUES DDOS SEGÚN ESTRATEGIA DE SATURACIÓN.

- La saturación de la víctima puede ser:
  - Del ancho de banda
    - Nivel de red/transporte (OSI)
  - De los recursos del servidor (capa 7)
    - Orientada a consumir CPU y memoria
    - Caída de equipos de red, servidores,…
    - Nivel de aplicación (OSI)
- La estrategia orientada a:
  - Explotación de vulnerabilidades
    - Búsqueda de acceso a la infraestructura
    - Robo de datos
      - Mediante cortinas de humo

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

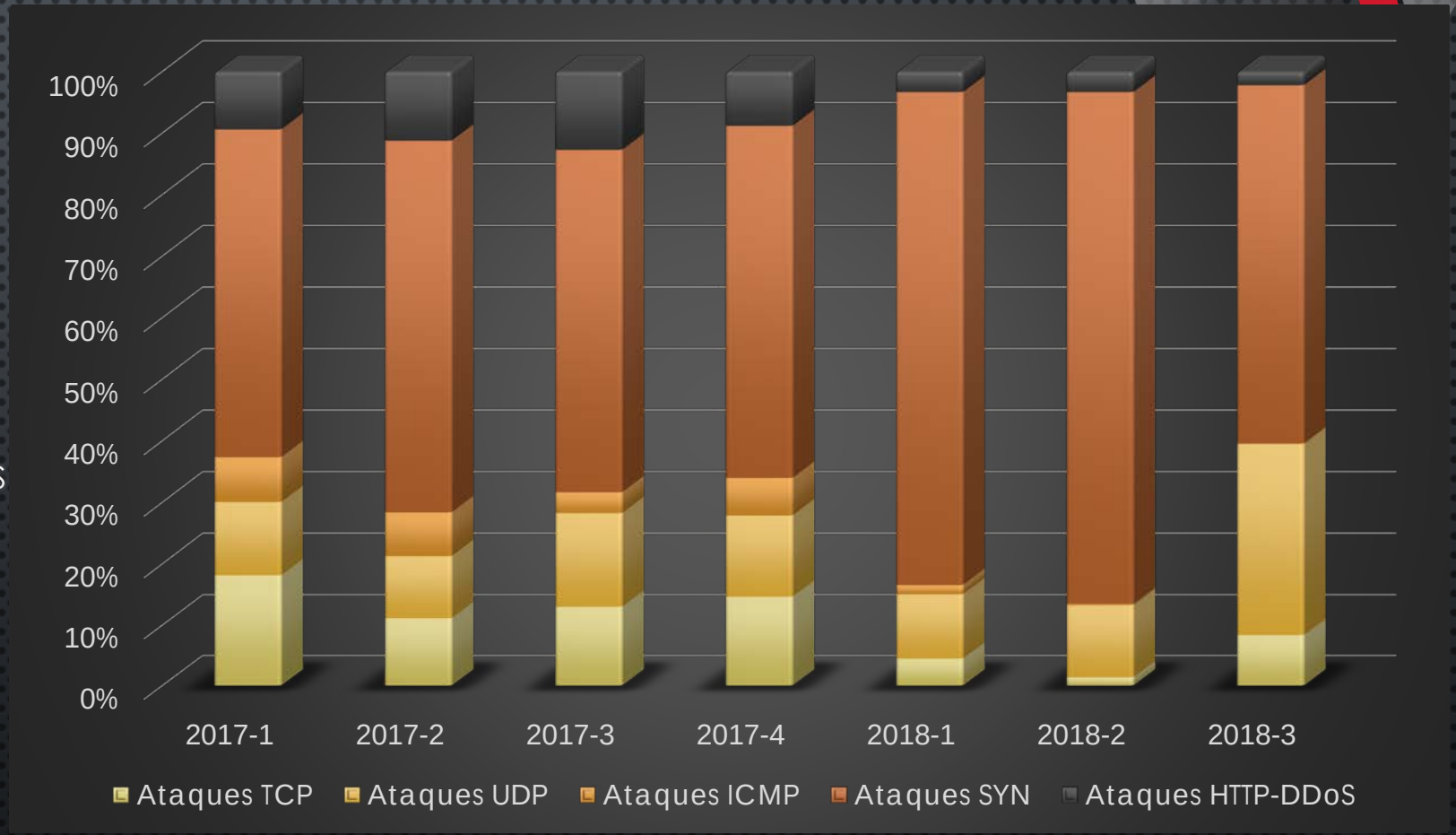
VNiVERSiDAD D SALAMANCA 1218 - 2018

SICPD Servicios Informáticos CPD

UNIDAD DE SERVIDORES DE SISTEMAS

INFORMES ANUALES (SECURE LIST).

- La mayoría SYN
- Crecimiento de los UDP
- Variación HTTP-DDoS
  - En función de tools
  - No depende de botnets
    - Desde pocos equipos
  - Combinados
    - Exploits de webs

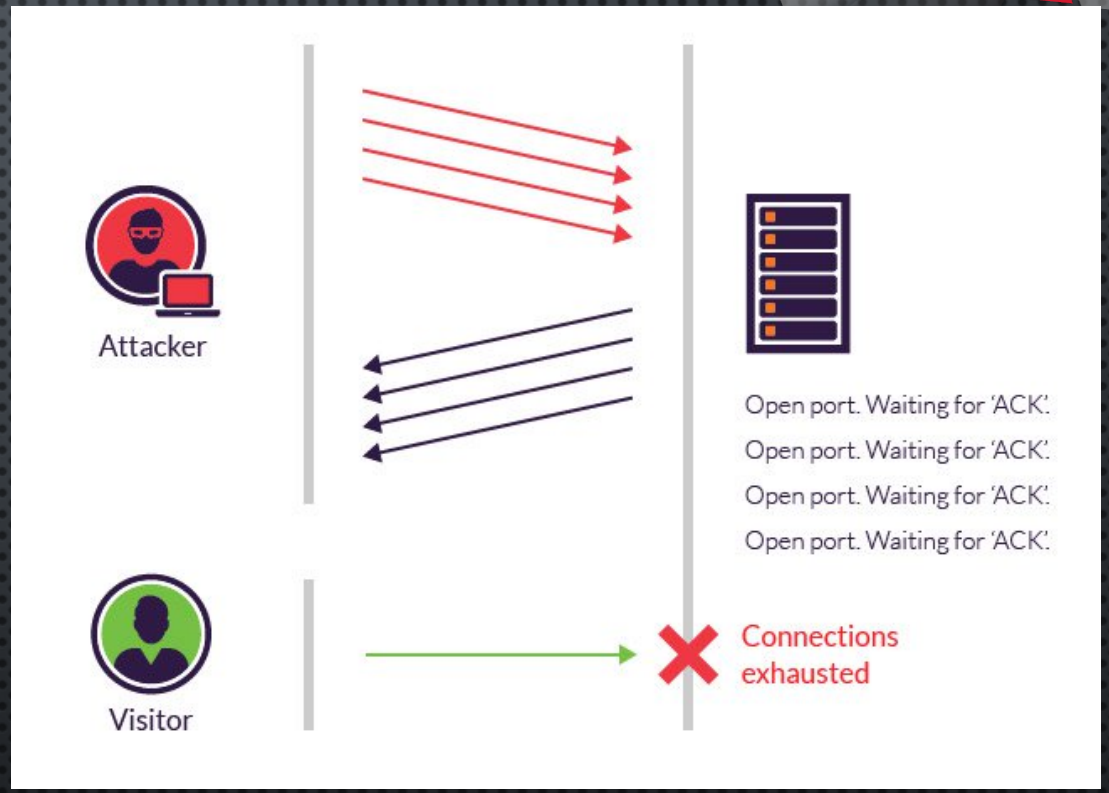


UNIDAD DE SERVIDORES DE SISTEMAS

MODELOS DE ATAQUE: TCP SYN FLOOD.

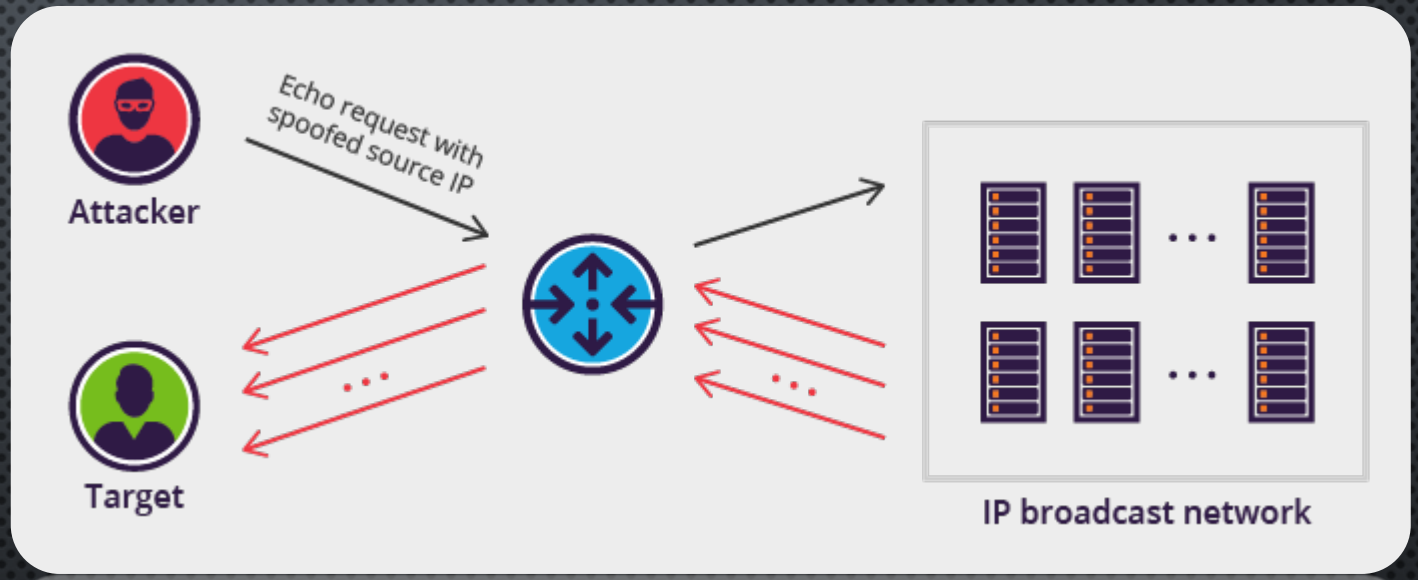
- Saturación de protocolo (layer 4)
- Procedimiento sencillo:
  - El atacante inicia varias señales SYN
  - La víctima le devuelve SYN+ACK
    - Un cliente debería de iniciar conexiones
  - El atacante no manda datos
  - La víctima acaba saturada de abrir puertos para esperar datos que no llegan nunca.
- Fácil de ejecutar:

```
$ hping3 -p 80 -S --flood IP_víctima
```



MODELOS DE ATAQUE: ICPM FLOOD.

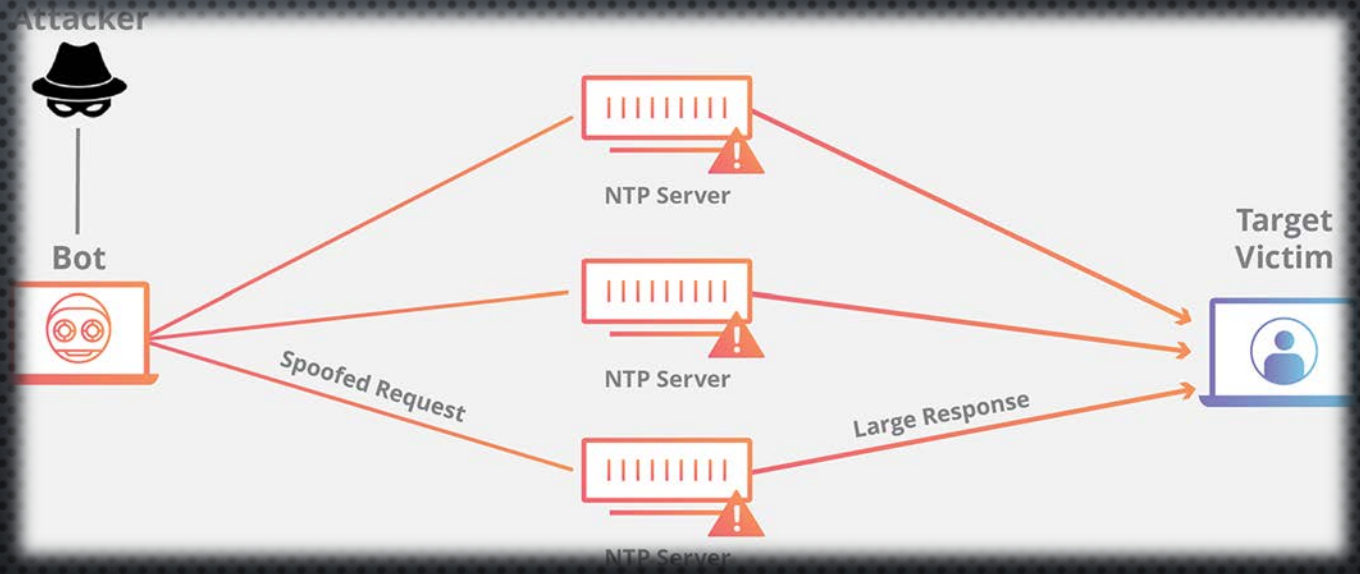
- Varios tipos
  - Ping flood
  - Smurf Attack (pitufo)
- Cambio de IP de respuesta
  - Múltiples peticiones ICMP
    - Peticiones "rápidas"
  - Respuesta a la víctima
    - Saturación de la víctima
- Evitarlos
  - Segmentación de red
  - Bloqueo por fw perimetral
  - Bloqueo de ICMP localmente



UNIDAD DE SERVIDORES DE SISTEMAS

MODELOS DE ATAQUE: NTP AMPLIFICADO.

- Fallo o mala configuración NTPd
  - Versiones anteriores a 4.2.17
- El atacante envía consultas NTP
  - De monitorización
  - A diversos servidores
  - Cambia (spoof) la IP de respuesta
    - Por la de la víctima
  - Todo el mundo responde...
    - A la víctima
- Se refleja el tráfico x20, x200...



UNIDAD DE SERVIDORES DE SISTEMAS

ATAQUES HTTP-DOS.

- Slow headers (Sloworis)
  - Cabeceras HTTP incompletas
  - Sin CR+LF final
- Slow HTTP post body
  - En base a la cabecera content-length
    - Envía menos bytes… espera más
- Apache Killer (el más común)
  - Muchas peticiones superpuestas
- Slow Read
  - Retardo al enviar los ACKs (HTTP)

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

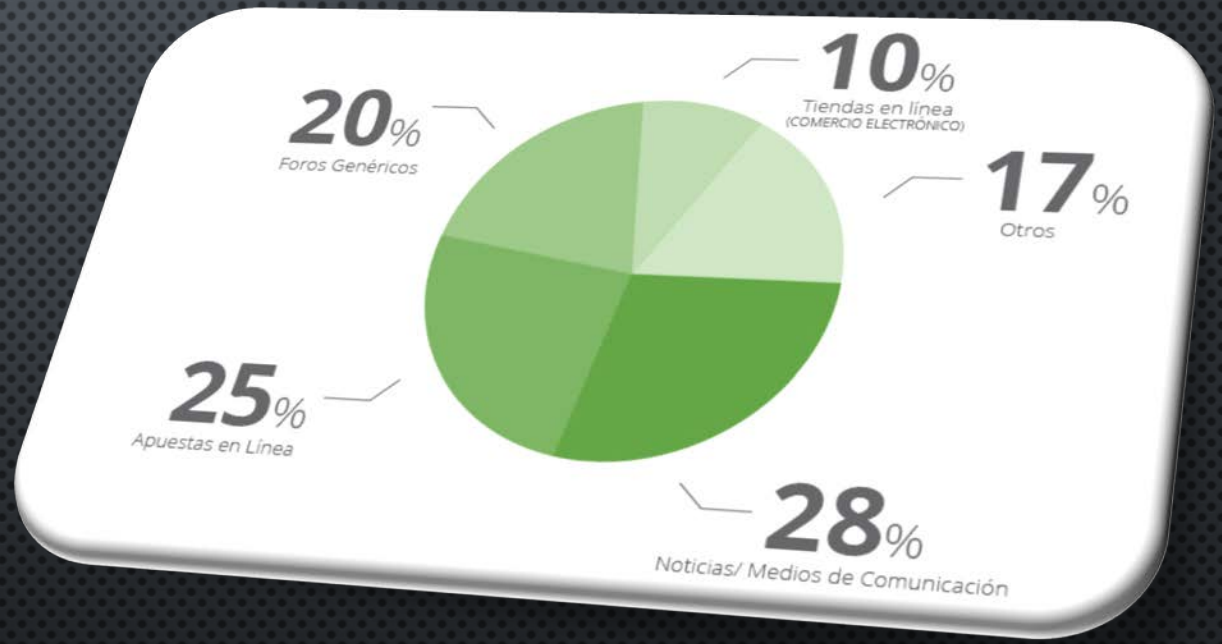
VNiVERSiDAD D SALAMANCA
1218 - 2018

SICPD
Servicios Informáticos
CPD

UNIDAD DE SERVIDORES DE SISTEMAS

ATAQUE HTTP-FLOOD (I).

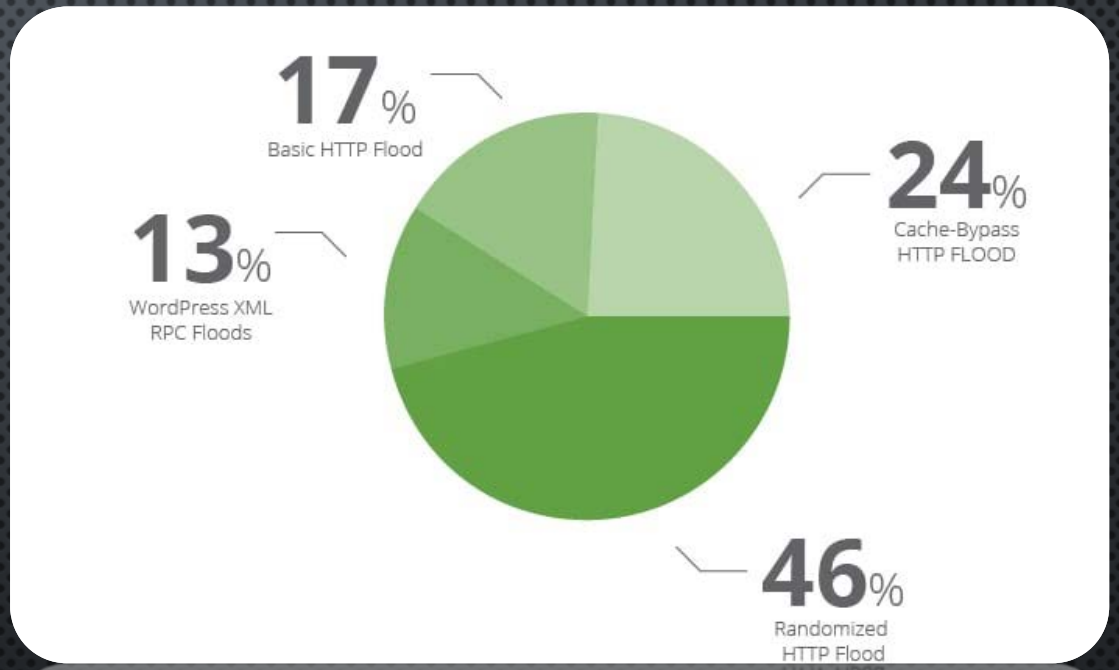
- Peticiones contra aplicaciones.
- Aprovechar scripts de mayor carga
  - Recorrido en la base de datos grande
  - Carga de datos no indexados
- Ejemplo de las URLs cortas
  - URLs cortas inventadas
  - Continua búsqueda en la base de datos
- Peticiones rápidas en modo HEAD



UNIDAD DE SERVIDORES DE SISTEMAS

ATAQUE HTTP-FLOOD (Y II).

- Fases de un HTTP Flood
  - Solicitud de URLs desde IPs distintas
    - Uso de botnets
    - Métodos GET, POST y HEAD
      - HEAD es rápido para hacer la solicitud
      - No se espera la respuesta
    - Peticiones de ejecución de script pesado
      - Ejecución de búsquedas
        - Operación de largo recorrido
      - Parámetro http://x.y.z/?s=12343
- Carga de memoria y de CPU en el servidor



VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

VNiVERSiDAD D SALAMANCA
1218 - 2018

SICPD
Servicios Informáticos
CPD

UNIDAD DE SERVIDORES DE SISTEMAS

RADIOGRAFÍA DE UN ATAQUE HTTP-DOS (I).

- Combinación de ataque
  - Ataque NTP amplificado
    - 14,5 Gbps
    - Detenido por RedIris Egida
  - Ataque HTTP-DOS
    - Cuestión de análisis y de estudio
    - Múltiples solicitudes Head
    - Múltiples remitentes: Ucrania, China…
    - 3.500 request per minute de URL falsa:
      - http://x.y.z/biblioteca
      - Al no parecer extraña, no nos "cantó" inicialmente
    - Devolución de un 404
      - 3.500 búsquedas ppm y devoluciones de un 404

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

VNiVERSiDAD D SALAMANCA 1218 - 2018

SICPD Servicios Informáticos CPD

UNIDAD DE SERVIDORES DE SISTEMAS

RADIOGRAFÍA DE UN ATAQUE HTTP-DDOS (II).

- Prueba del ataque: 15 de febrero
  - La relizan 2 días antes
  - 3285 ataques desde 11 Ips distintas
    - Caída del servidor un par de horas
- Ataque "en directo": 17 de febrero
  - Desde 816 subredes distintas
    - 213 de China
    - 125 de Rusia
    - 83 de Indonesia
    - 58 de Brasil
    - 37 de Ucrania
    - 36 de Bangla Desh
    - 34 de Thailandia

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

VNiVERSiDAD D SALAMANCA
1218 - 2018

SICPD
Servicios Informáticos
CPD

UNIDAD DE SERVIDORES DE SISTEMAS

RADIOGRAFÍA DE UN ATAQUE HTTP-DDOS (Y III).

- Análisis en el log
  - Necesidad de obtener las Ips de:
    - Patrones 404 altamente repetitivos
      - Miles de solicitudes de la misma URL
      - Desde Ips origen distintas
        - Obtención de subredes en Whois
        - No sirve bloquear una sóla IP
  - Extraer log de respuestas 404
    - De forma independiente
    - Facilita el análisis
  - Problema si hay fallos (favicon, imagen...)
- Bloqueamos a todo el mundo

- Detención de atacantes
  - Por aplicación: CMS (fallido)
    - Tarda en rechazarlas
    - Tiene que analizarlas
  - Por el FireWall local Iptables
    - Altamente eficiente
    - Necesidad de diálogo con el web
      - Fail2ban
      - Análisis de logs (scripts)

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

VNiVERSiDAD D SALAMANCA
1218 - 2018

SICPD
Servicios Informáticos
CPD

UNIDAD DE SERVIDORES DE SISTEMAS

EXPLICACIÓN DEL ATAQUE (I).

- Problema de los aplicativos web: vulnerables
  - Abiertos a toda internet por HTTP/HTTPS
  - Mantenimiento de conexiones: KeepAlive
    - Gasolina al fuego
  - Sin comprobación de cierre de conexiones
    - Saturación del Pool de conexiones
  - Aceptación de HEAD
- Detecciones desde el WAF
  - No las detecta... son peticiones "legales"

UNIDAD DE SERVIDORES DE SISTEMAS

EXPLICACIÓN DEL ATAQUE (Y II).

- Requerimientos para un ataque HTTP-DOS
  - No necesita mucho ancho de banda
    - Muchas peticiones, no espera respuesta
  - Mínimos recursos
    - Poco ancho de banda (WiFis públicas)
    - Poca CPU/mem (Android, RPi,...)
- Mantenimiento de un ataque
  - Mientras esté encendido
    - Redes de BOTs
- Peticiones HTTP (más fáciles) vs HTTPS
  - Redirect forzado al navegador
    - No a un script (de python, java...)
- Abuso de las short-URLs (facilita el ataque)
  - Basta con hacer peticiones de URLs que no existen
  - Tendrán que buscar la la coincidencia en toda la base de datos
    - Carga al servidor

UNIDAD DE SERVIDORES DE SISTEMAS

ESTRATEGIA DE PROTECCIÓN.

- Configuración segura de servidores
- Parcheo y actualización del software
- Ajustes en los Firewalls
- Instalación "fina" de un WAF
- Servicios redundados y balanceados
- Estratificación en capas
- Control de intentos de login
  - Captchas y Estadísticas de "brute-force attemps"
- Antivirus
- Análisis de contenido en busca de fallos
- Plan de emergencia
- Estaticidad del sitio web

UNIDAD DE SERVIDORES DE SISTEMAS

PROTECCIÓN EN EL SERVIDOR WEB.

- Paremetrización del servidor (WebServer y FW)
  - Indicar el máximo de conexiones por IP (Evasive)
  - Limitar la duración de una conexión
  - Limitar el ancho de banda por IP (QoS, BandWidth)
  - Máximo número de conexiones por segundo desde una IP
- Implementación de un WAF (modSecurity)
- Redundancia y Balanceo de carga
- División en capas
  - Proxy NGINX + Apache
- Charlas con el Firewall (fail2ban…)
  - Más efectivo al no llegar al servidor ineficiente

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

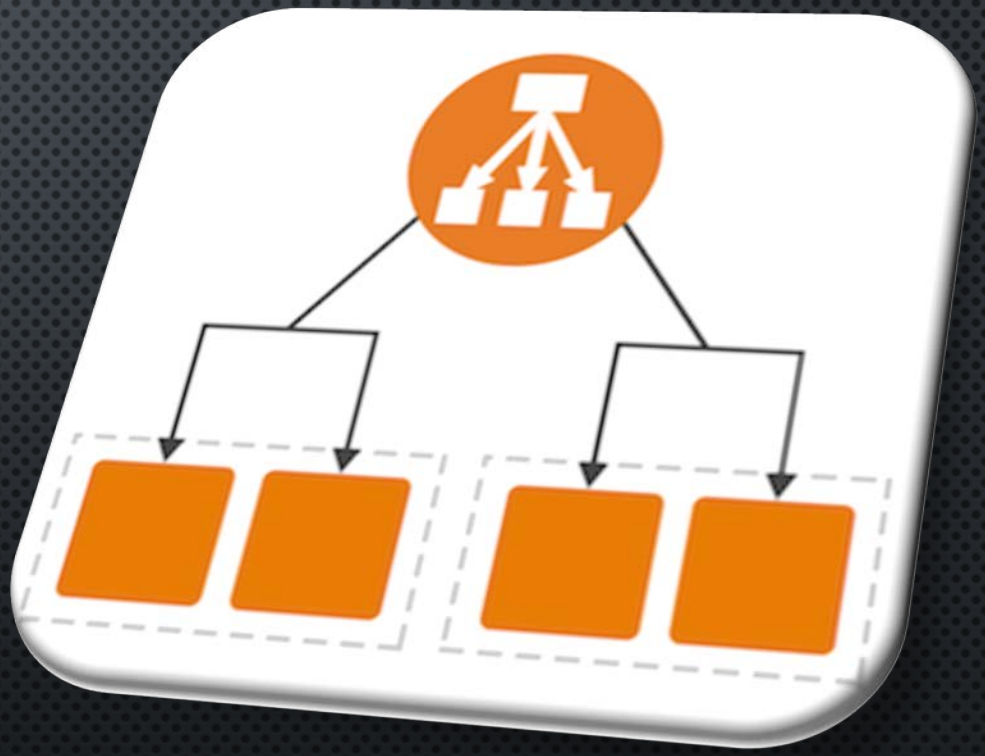
VNiVERSiDAD D SALAMANCA
1218 - 2018

SICPD
Servicios Informáticos
CPD

UNIDAD DE SERVIDORES DE SISTEMAS

REDUNDANCIA Y BALANCEO.

- El problema de tener un sólo servidor
  - Todos los ataques van contra él
  - No hay alternativa si cae
- El balanceo de carga distribuye el ataque
  - Objetivo de distribuir equitativamente el ataque
    - Reduce el impacto por servidor
  - Importante la gestión de sesión en el balanceador
    - Reparto por carga o round-robin con sticky
      - Un "sticky" relativamente bajo
      - En caso contrario, los tirará de 1 en 1



UNIDAD DE SERVIDORES DE SISTEMAS

CONFIGURACIÓN DEL FIREWALL.

- PREPARACIÓN DEL SISTEMA
  - VARIABLES SYSCTL NET.IPV4.TCP_...
    - SYNCOOKIES
    - FIN_TIMEOUT
    - WINDOW_SCALING
    - SACK
- LIMITACIÓN EN EL FIREWALL
  - SIEMPRE MÁS EFICIENTE QUE EN NINGÚN OTRO SITIO
  - NO LLEGA A PEDIR APLICACIÓN NI CONEXIÓN WEB

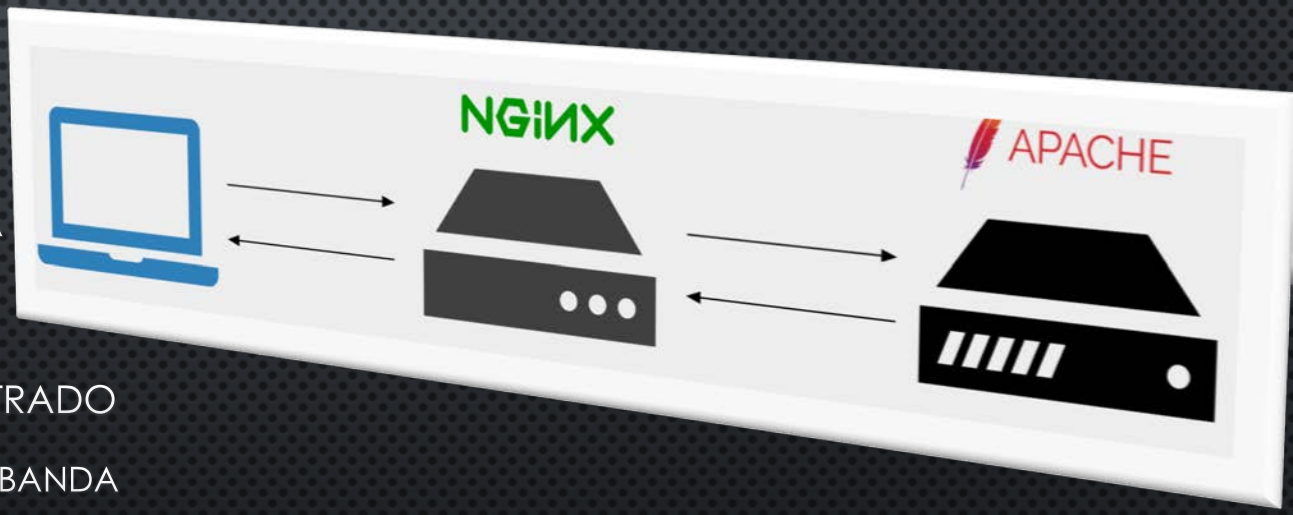
```
--syn --dport 80 -m connlimit --connlimit-above 20 -j REJECT --reject-with tcp-reset
```

```
-m state --state NEW -m recent -update --seconds 30 --hitcount 20 --name DEFAULT -j DROP
```

UNIDAD DE SERVIDORES DE SISTEMAS

DIVISIÓN EN CAPAS.

- Servicio más extendido: Apache + PHP
  - Apache no gestiona eficientemente las request/connections
    - Lento y póco ágil
  - Uso (y abuso) del Keep-Alive
    - Más leña al fuego
    - Consumo alto de recursos de memoria
- Añadir NGINX como proxy inverso
  - Mejora la gestión de peticiones y su filtrado
    - IP/subred, geolocalización, ancho de banda
    - Agentes, número de peticiones, WAF



UNIDAD DE SERVIDORES DE SISTEMAS

APLICACIÓN DE LEGISLACIÓN.

- Modificación del código penal por **LO 1/2015** (3/2015)
  - Artículos 575.1 575.2 197 bis 1, 197 bis 2, 246C y 246 bis C del Código Penal
  - Aplicación dentro del marco europeo
    - Directiva 2013/40 UE del 12 de agosto de 2013 del parlamento europeo
    - Sustituye el marco 2005/222 del 24 de febrero de 2005 (ataques contra sistemas de información)
- Principales delitos:
  - Interceptación de transmisiones (197 bis apartado segundo)
  - Facilitación para el anterior (197 ter)
  - **Sabotaje informático** (263)

UNIDAD DE SERVIDORES DE SISTEMAS

MUCHAS GRACIAS...

Juan Antonio González Ramos
juanan@usal.es

JORNADAS TÉCNICAS RedIRIS
30 edición
28-30 MAYO 2019
SEVILLA

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

VNiVERSiDAD D SALAMANCA
1218 - 2018

SICPD Servicios Informáticos CPD